THE SEDONA CONFERENCE COMMENTARY ON INFORMATION GOVERNANCE * *-- A Project of The Sedona Conference Working Group on Electronic Document Retention & Production (WG1)*

Fall, 2014

Reporter
15 Sedona Conf. J. 125

Length: 19272 words

Author: Author: The Sedona Conference Editor-in-Chief Conor R. Crowley Drafting Team Keith M. Angle and Jason R. Baron and Christopher Beahn and Bennett B. Borden and Howard Feldman and Liam A. Ferguson and Dean Gonsowski and Jack Halprin and Tim Hart and Virginia H. Johnson and Wayne C. Matus and Tim Noonan and Cheryl Pederson and Charles R. Ragan and Jim Shook and Peter Sloan and David L. Stanton and Cheryl Strom and Jeane A. Thomas

Highlight

Thanks go to all who participated in the dialogue that led to this Commentary. We thank all of our Working Group Series Sustaining and Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors just click on the "Sponsors" Navigation bar on the homepage of our website.

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 1. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any other organizations to which any of the participants belong, nor do they necessarily represent official positions of The Sedona Conference.

Text

PREFACE

Welcome to The Sedona Conference *Commentary on* ***Information Governance***, a project of The Sedona Conference Working Group One on Electronic Document Retention & Production (WG1). WG1 is best known for its ground-breaking publication, *The Sedona Principles* Addressing Electronic Document Production, and as such, is generally associated in the minds of legal professionals and the public at large with civil litigation, and more specifically, with electronic discovery. But when *The Sedona Principles* were being drafted ten years ago, members of WGI immediately recognized that no discussion of electronic discovery in civil litigation was complete, or even possible, without a discussion of the records and ***information*** management context from which requests for and responses to electronic discovery emanate. As a consequence, *The Sedona Principles* have been augmented over the past decade by WGI commentaries that discuss the management of electronic ***information*** in the day-to-day conduct of business, government, and private life. These commentaries have included:

. *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing* ***Information*** *& Records in the Electronic Age*
. *The Sedona Conference Commentary on Email Management*
. *The Sedona Conference Commentary on Inactive* ***Information*** *Sources*

. *The Sedona Conference Primer on Social Media*
. *The Sedona Conference Best Practices Commentary on Search & Retrieval Methods*
. *The Sedona Conference Commentary on Finding the Hidden ROI in **Information** Assets*

With the exception of the final title in the above list, one could still sense in all these commentaries that the litigation risk management tail might be wagging the ***information*** management dog. The final Commentary on *Finding the Hidden ROI in **Information** Assets* broke cleanly with that history, initiating a discussion that went beyond managing the e-discovery risks associated with ***information***, to better leverage the enormous value of ***information*** that is caught up within firms and organizations of all types.

We now take the next step, and that is to define ***Information Governance*** as an organization's coordinated, interdisciplinary approach to satisfying ***information*** compliance requirements and managing ***information*** risks while optimizing ***information*** value. In drafting this Commentary, it has been the mission of WGI to bring together lawyers, records and ***information*** managers, technical experts, privacy and security professionals, business process engineers, human resource officers, and others, to develop a comprehensive set of basic principles to guide the development and operation of a robust ***Information Governance*** program in any organization.

The Commentary represents the collective efforts of many individual contributors. On behalf of The Sedona Conference, I wish to thank everyone involved in devoting their time and attention during the drafting and editing process, and in particular Keith Angle, Jason Baron, Dean Gonsowski, Tim Hart, Wayne Matus, Cheryl Pederson, Chuck Ragan, Jim Shook, Peter Sloan, David Stanton, and Cheryl Strom. I especially acknowledge the tireless evangelism of Editor-in-Chief Conor R. Crowley, who not only spent countless hours on the draft of this Commentary but also patiently explaining the concept of ***Information Governance*** to sometimes resistant stakeholders, helping them break out of their professional "silos" and recognize the need for a broader vision.

The Commentary represents the collective wisdom of a score of highly-qualified ***Information Governance*** professionals who contributed to the draft. The members of The Sedona Conference Working Group Series were able to review and comment on this Commentary prior to publication, it was presented at the 2013 Georgetown Law Center eDiscovery Institute, and it benefited from a six-month public comment period. But ***Information Governance*** is still very much an evolving concept. The drafters and contributors all agree that through shared experience and dialogue, ***Information Governance*** will mature as a discipline, necessitating a second edition of this Commentary. You are invited to join the dialogue online at *https://thesedonaconference.org* or submit comments by email to *info@sedonaconference.org*.

Kenneth J. Withers
Deputy Executive Director
The Sedona Conference
October 2014

THE SEDONA CONFERENCE PRINCIPLES OF ***INFORMATION GOVERNANCE***

1. Organizations should consider implementing an ***Information Governance*** program to make coordinated decisions about ***information*** for the benefit of the overall organization that address ***information***-related requirements and manage risks while optimizing value.

2. An ***Information Governance*** program should maintain sufficient independence from any particular department or division to ensure that decisions are made for the benefit of the overall organization.

3. All ***information*** stakeholders should participate in an organization's ***Information Governance*** program.

4. The strategic objectives of an organizations ***Information Governance*** program should be based upon a comprehensive assessment of ***information***-related practices, requirements, risks, and opportunities.

5. An ***Information Governance*** program should be established with the structure, direction, resources, and accountability to provide reasonable assurance that the program's objectives will be achieved.

6. The effective, timely, and consistent disposal of physical and electronic ***information*** that no longer needs to be retained should be a core component of any ***Information Governance*** program.

7. When ***information governance*** decisions require an organization to reconcile conflicting laws or obligations, the organization should act in good faith and give due respect to considerations such as privacy, data protection, security, records and ***information*** management, risk management, and sound business practices.

8. If an organization has acted in good faith in its attempt to reconcile conflicting laws and obligations, a court or other authority reviewing the organization's actions should do so under a standard of reasonableness according to the circumstances at the time such actions were taken.

9. An organization should consider reasonable measures to maintain the integrity and availability of long-term ***information*** assets throughout their intended useful life.

10. An organization should consider leveraging the power of new technologies in its ***Information Governance*** program.

11. An organization should periodically review and update its ***Information Governance*** program to ensure that it continues to meet the organization's needs as they evolve.

EXECUTIVE SUMMARY

Information is crucial to modern businesses. ***Information*** can have great value, but also pose great risk, and its ***governance*** should not be an incidental consideration. Despite these realities, there is no generally accepted framework, template, or methodology to help organizations make decisions about ***information*** for the benefit of the organization rather than any individual department or function.

"***Information Governance***" as used in this Commentary means an organization's coordinated, inter-disciplinary approach to satisfying ***information*** compliance requirements and managing ***information*** risks while optimizing ***information*** value. As such, ***Information Governance*** encompasses and reconciles the various legal and compliance requirements and risks addressed by different ***information***-focused disciplines, such as records and ***information*** management ("RIM"), [1] data privacy, [2] ***information*** security, [3] and e-discovery. [4] Understanding

---

[1] **Records and *Information* Management** is the standardized process to create, distribute, use, maintain and dispose of records and ***information***, regardless of media, format or storage location, in a manner consistent with an organization's business priorities and applicable legal and regulatory requirements. RIM principles also provide for the temporary suspension of policies or processes that might result in the deletion of records or ***information*** subject to a legal hold.

See generally, S. Soares, *Selling **Information Governance** to the Business: Best Practices by Industry and Job Function* (2011) (providing insight into the best ways to encourage businesses to implement an ***information governance*** program).

[2] **Data Privacy** is the right to control the collection, sharing and destruction of ***information*** that can be traced to an individual. In general, data privacy is more comprehensively protected outside of the United States, particularly in the European Union member states, where the Data Protection Directive provides significant restrictions on the processing and transfer of personal data, and other countries including Argentina, Canada, Israel, Switzerland and Uruguay. *See* Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJL 281/31. In the US, the approach to data privacy is generally contractual, and does not enjoy the same level of generic legal protections. Disparate laws in the United States do, however, mandate protections for specific types of data or target different groups. Examples include: patient records under the Health Insurance Portability and Accountability Act ("HIPAA"), financial ***information*** under the Graham-Leach-Bliley Act ("GLBA"), and prohibitions on the collection of ***information*** about children younger than 13 years old, under the Children's Online Privacy Protection Act ("COPPA").

See Gartner, *"First 100 Days: Enterprise Content Management Initiatives"* (July 7, 2011), *available at* *http://www.gartner.com/id=1739415*.

[3] ***Information* Security** is the process of protecting the confidentiality, integrity, and availability of ***information*** and assets, enabling only an approved level of access by authorized persons, and properly disposing of such ***information*** and assets when

the objectives of these disciplines allows functional overlap to be leveraged (if synergistic); coordinated (if operating in parallel); or reconciled (if in conflict). [5]

The position of The Sedona Conference is that ***Information Governance*** should involve a top-down, overarching framework, informed by the ***information*** requirements of all ***information*** stakeholders that enable an organization to make decisions about ***information*** for the good of the overall organization and consistent with senior managements strategic directions.

This paper explains the need for a comprehensive approach to ***Information Governance***. The paper addresses:

. Why traditional, siloed approaches to managing ***information*** have prevented adequate consideration of ***information*** value, risk, and compliance for the organization as a whole;

. How hard costs, soft costs, opportunity costs, and risk accumulate for organizations lacking adequate control of ***information***;

. The definition of ***Information Governance***, its fundamental elements, and the resulting benefits to the organization; and

. The crucial role of executive sponsorship and ongoing commitment.

THE ***INFORMATION GOVERNANCE*** IMPERATIVE

We live and work in an ***information*** age that is continually -- and inexorably -- transforming how we communicate and conduct business. Regardless of an individual organization's size, mission, marketplace or industry, ***information*** is a crucial asset for all organizations; and if inadequately controlled, a dangerous source of risk and liability.

Some examples illustrate the highly public repercussions of ***information*** control lapses:

. Significant and increasing costs of complying with e-discovery obligations;

. Data privacy and security breaches, such as a global electronics company attributing $ 171 million in out-of-pocket remediation costs to a data breach affecting 100 million persons, with the total harm, including reputational injury, estimated to exceed $ 1 billion; [6]

---

required or when eligible. ***Information*** security often focuses on limiting access to certain types of ***information*** that is important to the organization by restricting access through various controls including physical safeguards, technical access controls (e.g., permissions to Read, Write, Modify, Delete, Browse, Add, and Rename), authorization challenges (e.g., usernames and passwords) and encryption technologies. Security requirements can be mandated by law (e.g., HIPAA Security Rule), by contract, by industry requirements (e.g., PCI) or simply by company requirements and best practices.

See, e.g., Soares, *supra*, at 149.

[4] **Electronic Discovery** ("e-discovery") is the process of identifying, preserving, collecting, preparing, analyzing, reviewing, and producing electronically stored ***information*** ("ESI") relevant to pending or anticipated litigation, or requested in government inquiries. E-discovery includes gathering ESI from numerous sources, reviewing and analyzing its relevance and the applicability of any privileges or protections from disclosure, and then producing it to an outside party.

As another example, it has been reported that one manufacturing company discovered and eliminated 37 unique definitions of "customer" across its enterprise, and agreed on a single, standard definition. Robert Routzahn, *"Business and IT Collaboration: Essential for Big Data* ***Information Governance****,"* IBM Data Magazine, (July 5, 2013), *http://ibmdatamag.com/2013/07/business-and-it-collaboration-essential-for-big-data-**information-governance**/*.

[5] *See* Appendix A for additional discussion of the intersections of these disciplines.

See, e.g., "The Sedona Conference Commentary on Finding the Hidden ROI In ***Information*** *Assets"*, The Sedona Conference, (Feb. 2011), *https://thesedonaconference.org/download-pub/466*.

. E-discovery sanctions, such as an award of $ 8.5 million in monetary sanctions against patent holder for willfully failing to produce tens of thousands of discoverable documents; [7]

. Recordkeeping compliance penalties, such as a national clothing retailer fined over $ 1 million by the U.S. Immigration and Customs Enforcement Agency for ***information*** compliance deficiencies in its I-9 employment verification system, and a retail pharmacy chain reaching an $ 11 million settlement with the U.S. Government for record-keeping violations under the Controlled Substances Act. [8]

Behind the headlines, however, is a more pervasive problem -- the commonly unmeasured aggregation of hard costs, soft costs, opportunity costs, and risk borne by organizations that fail to effectively control their ***information***.

Knowingly or not, organizations face a fundamental choice: they can control their ***information***, or by default, they can allow their ***information*** to control them.

Siloed Approaches Fail to Govern *Information*

Many organizations have traditionally used siloed approaches when managing ***information***, resulting in decisions being made without sufficient consideration of ***information*** value, risk, or compliance for the organization as a whole. Examples of these silos include the various departments or administrative functions within the organization that deal with the organization's ***information***, such as IT, Legal, Compliance, Records and ***Information*** Management, HR, Finance, and the organization's various business units. Each business unit or administrative function commonly has its own ***information governance*** policies and procedures, as well as disparate data systems and applications.

Another type of ***information*** silo consists of those disciplines that deal with specialized categories of ***information*** issues, such as data privacy and security (focused on protection of regulated classes of ***information***), litigation e-discovery (focused on preservation and production of ***information*** in litigation), and data ***governance*** [9] (focused

---

[6] Mathew J. Schwartz, *Sony Data Breach Cleanup to Cost $ 171 Million*, ***INFORMATION*** WEEK SECURITY, May 23, 2011, *http://www.informationweek.com/security/attacks/sony-data-breach-cleanup-to-cost-171-mil/229625379*.

A medical device manufacturer estimated that improving ship-to addresses in a 100,000 item database could increase aftermarket sales by $ 1 million. Soares, *supra*, at 69.

[7] *Qualcomm, Inc. v. Broadcom Corp.*, No. 05cvl958- *B (BLM), 2008 WL 66932* (N.D. Cal. January 7, 2008) *vacated in part by* Qualcomm v. Broadcom Corp., No. 05 CV1958-RMB (BLM), 2008 WL 638108 (N.D. Cal. March 5, 2008); *see also Day v. LSI Corp.*, No. CIV 11-186- TUC--CKJ, 2012 WL 6674434 (D. Ariz. Dec. 20, 2012) (awarding partial default judgment *a document retention policy and a litigation hold that was not properly enforced); Pillay v. Millard Refrigerated Servs., Inc.*, No. 09 C 5725, *2013 WL 2251727* (N.D. Ill. May 22, 2013) (issuing adverse inference instruction against a company for and attorney's fee award of $ 10,000, resulting from the loss of ***information*** that should have been retained according to both foiling to stop the automatic deletion of employee productivity tracking data, which it had used as a reason for terminating a disabled employee).

A recent Rand survey states that the review process alone averages $ 18,000 a gigabyte, meaning that with collection, preservation, hosting, etc., e-discovery costs can easily exceed $ 20,000 a gigabyte. Pace, Nicholas M. and Laura Zakaras. *Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery*. RAND Corporation, (2012), *http://www.rand.org/pubs/monographs/MG1208*. Also available in print form.

[8] Immigration and Customs Enforcement, Department of Homeland Security, *Abercrombie and Fitch Fined after I-9 Audit*, (2010), *http://www.ice.gov/news/releases/1009/100928detroit.htm* (last visited Nov. 13, 2013); Debbie Cai,*DOJ: CVS to Pay $ 11 Million to Settle Claims of Bad Record-Keeping*, THE WALL STREET JOURNAL, (April 3, 2013), *available at http://online.wsj.com/article/BT-CO-20130403-710237.html*.

[9] We recognize that various definitions of "***information governance***" have been advanced (*see e.g.*, Charles R. Ragan, ***Information Governance****: It's a Duty and It's Smart Business*, *19 RICH. J.L. & TECH. 12 at 30-33 (2013), available at http://jolt.richmond.edu/v19i4/article12.pdf*, and that there is an emerging discipline called "data ***governance***," and submit that data ***governance*** is a subset of our ***information governance*** concept. The Data ***Governance*** Institute, self-described as a mission-based and vendor neutral authority on essential practices for data strategy and ***governance***, defines "data

on ***information*** reliability and efficiency). Over time, these disciplines have developed their own terminologies and frameworks for identifying issues and addressing specific ***information*** challenges.

The core shortcoming of the siloed approach to governing ***information*** is that those within particular silos are constrained by the culture, knowledge, and short-term goals of their business unit, administrative function, or discipline. They perceive ***information***-related issues from the vantage point of what is familiar and important specifically to them. They often have no knowledge of gaps and overlaps in technology or ***information*** in relation to other silos within the organization. There is no overall ***governance*** or coordination for managing ***information*** as an asset, and there is no roadmap for the current and future use of ***information*** technology.

Siloed decisions concerning ***information*** often have unintended consequences for the organization as a whole, with significant cost and risk repercussions:

. An organization's individual business units independently make decisions about implementing ***information*** technology tools and systems, separate from the other business units. This results in duplication of technology and unneeded expense, and also prevents the efficient sharing of ***information***, a valuable asset, across the organization.

The IT Department establishes email account volume limits to relieve operational stress on an organization's email system. This results in personnel moving email to storage on local drives and devices, exacerbating both data security risks and difficulties in finding and preserving such email for litigation.

. Legal counsel issues overbroad litigation holds to avoid even a remote possibility of spoliation sanctions. This results in excessive costs in pending and future litigation and also the unnecessary retention of data.

. Personnel are allowed to conduct an organization's business on their own laptops and smartphones, under a Bring-Your-Own-Device ("BYOD") program to increase convenience and efficiency but without sufficient BYOD policies and controls or planning for natural attendant consequences. This results in data security exposures and difficulties in applying records retention policies and in preserving and collecting data for litigation.

. Privacy and data security controls are applied to an organization's service providers, but are not used to ensure that service providers also meet the organization's records retention requirements. This may result in inconsistent application of such requirements to records.

. Records manager initiates a robust data and email retention program without regard to potential technological limitations or the burden associated with retaining, searching and reviewing the resulting data for e-discovery purposes.

In the post-Sarbanes-Oxley world, many companies have adopted codes of conduct, in which they broadly proclaim that the organization and its employees comply with all applicable laws (including privacy and data security requirements), protect confidential ***information***, use electronic communications wisely, and follow procedures for retaining records. The siloed approach to addressing ***information*** issues, however, inevitably spawns a multitude of ***information***-related policies adopted though various projects and initiatives. Thus, rather than a clear, uniform set of ***information*** policy guidance, employees face a cacophony of conflicting policies and procedures, making compliance virtually impossible in the heat of a competitive business environment, and negatively impacting productivity.

The "elephant in the room" is the organization's need to harness and control its ***information***, coupled with the inadequacy of a siloed approach for accomplishing this crucial goal. The solution to this quandary is for

---

governance" as "a system of decision rights and accountabilities for ***information***-related processes, executed according to agreed-upon models which describe who can take what actions with what ***information***, and when, under what circumstances, using what methods."*Definitions of Data* ***Governance***, THE DATA ***GOVERNANCE*** INSTITUTE, *http://www.datagovernance.com/adg_data_**governance**_definitions* (last visited Nov. 13, 2013). So viewed, "data ***governance***" does not address "why" an organization chooses to do certain things with its data and other ***information***; that is the critical role of ***Information Governance***, ensuring that actions users take win ***information***-related assets is consistent with organizational strategy.

organizations to find a way to bridge across their silos, so that issues of ***information*** compliance, risk, and value can be identified, understood, and addressed for the benefit of the entire organization.

Information Governance

"***Information Governance***" as used in this Commentary means an organization's coordinated, inter-disciplinary approach to satisfying ***information*** legal and compliance requirements and managing ***information*** risks while optimizing ***information*** value. Organizations that adopt ***Information Governance*** programs are able to bridge across silos, thereby perceiving and understanding ***information***-related issues from the perspective of the overall organization. ***Information Governance*** also helps ensure that decisions and solutions regarding ***information*** compliance, risk controls, and value optimization will serve the needs of the entire organization rather than the insular needs of individual silos.

To accomplish ***Information Governance***, organizations should:

. Establish a structure for ***Information Governance***, which will vary in form depending on the organization's size, complexity, culture, and industry and regulatory environment;

. Determine the organization's strategic objectives for ***Information Governance***, based upon a comprehensive assessment of ***information***-related practices, requirements, risks, and opportunities;

. Reconcile the various compliance requirements and risks addressed by different ***information***-focused disciplines, such as records and ***information*** management, privacy, data security, and e-discovery; and

. Implement an ***Information Governance*** program with the structure, direction, resources, and accountability to provide reasonable assurance that the program's strategic objectives will be achieved.

The Benefits of *Information Governance* are Significant

The advantages of establishing an ***Information Governance*** program are many and varied, depending upon the ***information***-related issues and risks an organization faces. Beyond addressing the risks above, an enterprise-wide ***Information Governance*** program will help organizations achieve the following advantages, all of which add to the bottom line:

. Business performance improvements, as users gain confidence that they can locate valuable ***information*** efficiently and reliably, and better understand how to address ***information***-related risks;

. Realization of "option value" as the organization leverages existing ***information*** and technologies across diverse business units, consolidates technologies and administrative staff, and reduces license fees;

. More reliable and efficient processes and procedures for e-discovery;

. Reduced storage costs and administrative burdens, as obsolete and worthless ***information*** is eliminated; and

. Reduced costs and enhanced compliance with legal obligations for records retention, privacy and data security, and e-discovery, as ***information*** policies and processes are rationalized, integrated, and aligned in accord with the organization's ***information governance*** strategy.

Senior Leadership Support is Essential

The commitment of senior leadership is crucial for organizations to be successful in adopting ***Information Governance***. Such ongoing commitment is particularly important given the challenge of effectively bridging across existing organizational silos.

Thus, senior leadership should sponsor and firmly support the organization's ***Information Governance*** efforts by:

. Endorsing the importance of ***Information Governance*** to the entire organization;

. Chartering a structure of responsibility and accountability for implementing an ***Information Governance*** program;

. Adopting or approving the strategic objectives of the ***Information Governance*** program;

. Providing appropriate resources to implement and sustain the ***Information Governance*** program;

. Establishing a supportive "tone at the top" and an environment in which ***Information Governance*** remains an organizational priority; and

. Ensuring that the ***Information Governance*** program is administered consistent with its objectives and is periodically reviewed and updated.

There is often a balance of value against cost or risk that changes over time for a given ***information*** asset. Organizations may leverage ***information*** effectively over the short term, but once the data's short-term use is expended, the data is often stored away and rarely reassessed for any long-term strategic value. Left ungoverned, this potentially valuable asset is not only wasted, it also may become a significant liability. Through proper ***information governance***, organizations can realize additional benefit from their ***information*** assets over time while reducing risk.

The Business Case for *Information Governance*

Multiple business cases can be established for pursuing ***Information Governance***. Successful adoption of the ***information governance*** approach requires both strategic commitment (adoption of ***information governance*** as an organizational priority) and also tactical efforts (such as specific projects to establish and implement the program). A business case will be needed, both to support the strategic commitment and also to justify the expenditures of time, effort, and funding required for specific implementation projects. Because the business case for ***information governance*** must be persuasive at both strategic and tactical levels, the business case should include both strategic (qualitative) and project-based (quantitative, ROI) elements.

The Strategic/Qualitative Business Case:

Information governance is an ongoing program that evolves over time through maturity levels. As such, it is unrealistic to attempt to comprehensively quantify all of its benefits. One might just as easily attempt to exhaustively measure all benefits of managing the organization's tangible or people assets. ROI analysis is best used for applications of ***information governance*** to specific, issues or projects within the ***information governance*** initiative, as discussed in Appendix D.

At a strategic level, the business case should instead convey how ***information governance*** aligns with and amplifies the core values and fundamental, strategic objectives of the organization. For example:

. **Low Cost Provider**

Companies singularly focused on operational efficiency and cost control, such as in low-margin, high-volume industries or market segments, may adopt ***information governance*** to streamline ***information*** workflows and reduce unnecessary ***information*** storage and retention, thereby reducing costs and increasing business efficiency.

. **Innovative Excellence**

Organizations driven by creative innovation and excellence in products and services may adopt ***information governance*** to maximize the value of their ***information*** assets, helping them capture valuable ***information*** for innovative repurpose while minimizing the distraction of unnecessary ***information***.

. **Trusted Provider/Advisor**

Organizations with the core value and brand of being a trusted business provider or advisor may adopt ***information governance*** to strengthen their protection of ***information*** that customers or clients entrust to the organization and also to enhance third-party perceptions of the organization as a trusted custodian for such ***information***.

. **Integrity/Ethics**

Companies, including publicly traded organizations and those in highly-regulated industries, may adopt ***information governance*** as a complement to their internal control systems and corporate ethics and integrity programs to ensure ***information***-related legal compliance and risk management.

In each of the above examples, ***information governance*** provides specific, tangible benefits that often can be quantified on an ROI basis as discussed below. Yet, in each example, ***information governance*** also amplifies the organization's core value of choice, by ensuring that ***information*** is handled in alignment with the strategic value or brand. This alignment allows ***information governance*** to reinforce the particular organization's fundamental values, as ***information*** is managed in a way that "walks the walk."

Conversely, ***information governance*** also helps organizations avoid cultural dissonance for their core values, such as, for example, the "low cost provider" that squanders money on ***information*** inefficiency and unnecessary retention; the "innovative excellence" company that fails to optimize the value of its ***information***; the "trusted partner/provider" that is careless with the ***information*** entrusted to it; or the company espousing "integrity and ethics" that fails to establish a control environment for ***information*** as a valuable asset and as a means to detect and prevent compliance lapses. Thus, adoption of ***information governance*** can have profound, strategic significance beyond the quantitative ROIL measures mentioned below and considered in more detail in Appendix D.

The Quantitative/ROI Business Case:

A typical ROI analysis weighs the benefits of a particular project against its cost, and calculates the length of time it will take to recoup the cost. The quantitative aspects of the business case are best determined by focusing on specific applications of ***information governance*** to identified problems or opportunities, or to discrete projects for implementation of the ***Information Governance*** program. [10]

The quantifiable benefits from pursuing ***information governance*** generally fall into four main categories: optimizing corporate value, risk reduction, hard cost avoidance, and soft cost avoidance. See Appendix D for factors to consider when building a quantitative business case with these ROI categories.

THE SEDONA CONFERENCE PRINCIPLES OF ***INFORMATION GOVERNANCE***

Principle 1. Organizations should consider implementing an *Information Governance* program to make coordinated decisions about *information* for the benefit of the overall organization that address *information*-related requirements and manage risks while optimizing value.

Organizations benefit in several ways from managing ***information*** as a valuable asset. In order to realize these benefits, an ***Information Governance*** program should be established in a manner consistent with the organization's industry, compliance, and risk environments.

Any ***Information Governance*** program should incorporate the following principles: transparency, efficiency, integrity, accountability, and compliance. To be successful, the ***Information Governance*** program must be sponsored and firmly supported by the organization's senior leadership.

A core component of any ***Information Governance*** program should include a comprehensive data classification capability, combined with the effective, timely deletion of ***information***. By taking a comprehensive approach to identifying and addressing ***information***-related requirements, organizations can ensure compliance needs are met and conflicting issues are considered. It is also helpful to identify and assess ***information*** risks, such as user access control (***information*** security) and system failure (business continuity and disaster recovery), and ensure that such risks are understood so effective ***information*** controls can be put in place. This approach also aids in understanding ***information***-related strategic and operational objectives to help ensure that ***information*** value can be optimized without compliance lapses or uncontrolled risk.

---

[10] *See generally, S. Soares, Selling **Information Governance** to the Business: Best Practices by Industry and Job Function* (2011) (providing insight into the best ways to encourage businesses to implement an ***information governance*** program).

Although there are many stakeholders with divergent interests in managing ***information***, decisions about governing ***information*** should benefit the overall organization, rather than a particular department or discipline.

To enable an organization to make coordinated decisions about ***information*** for the benefit of the organization, the primary responsibility of an ***Information Governance*** program should be to create and maintain processes and procedures necessary for a coordinated, overall approach to decisions about ***information***. If agreement cannot be reached among stakeholders, the ***Information Governance*** program should provide a method for decisions to be made (subject to a challenge process) to enable the organization to move forward. Transparency, efficiency, integrity, accountability, and compliance are integral to the ability to perform this overall coordination and tie-breaking function successfully.

Responsible decision makers should use the ***Information Governance*** program at the time they make decisions about ***information***. Care should be taken to design the ***Information Governance*** program so that it can be used in this way. Existing ***governance*** mechanisms (such as budgetary ***governance*** or systems approval) may not be designed for users to interface with at the time decisions are being made. However, these can be leveraged or modified or new ones may be created, depending on an organization's circumstances.

Principle 2. An *Information Governance* program should maintain sufficient independence from any particular department or division to ensure that decisions are made for the benefit of the overall organization.

The ***information governance*** function must focus on the best interests of the organization. In order to fairly and effectively balance needs, however, the ***information governance*** program should have meaningful and balanced input from such departments as IT, legal, compliance, RIM, and the business units. One approach to accomplish this is to designate an executive who has sufficient independence to balance the competing needs of stakeholders rather than the interests of a single department. Ideally, the executive in charge of the ***Information Governance*** program reports at the same level as a General Counsel, CCO, CFO, or CIO. Another way to make decisions for the benefit of the overall organization is through a committee that has representation from impacted stakeholders, coupled with a process for elevating disagreements to a chief executive. Such a structure should be the ultimate goal for organizations with mature ***Information Governance*** programs. However, many organizations do not currently have in place any overarching ***information governance*** structure and their initial steps may include assigning ***information governance*** responsibilities to designated individuals within departments or lines of business. As this is not the optimal ***governance*** structure to reap the benefits of a coordinated approach to ***information governance***, organizations should strive for a structure that results in meaningful and balanced input from all impacted departments or divisions as their ***Information Governance*** programs mature. [11]

Many organizations have various departments (i.e., business units, IT, Legal, etc.) that take direction from a CEO or COO. Because goals differ across departments or functions, conflicts of interest may arise if the executive responsible for the ***Information Governance*** program reports to an individual stakeholder department.

An ***Information Governance*** program should ensure that decisions about ***information*** are made in the organization's best interests. Deciding for the overall good of the organization involves balancing the sometimes competing interests of many stakeholders. This balancing creates the potential that a given decision may not align with the particular objectives of a given department, particularly when the decision involves a balancing of cost and risk. For example, one stakeholder may believe a cloud-hosted service will reduce the cost of storing ***information***, but another may perceive an increased risk associated with the data being hosted in the cloud. The reduced cost may be attractive to a department such as IT, and the increased risk may be unattractive to another department such as Legal. In many cases, stakeholders can arrive at a mutually agreeable position that maximizes the benefit to the overall organization, for example by implementing mitigation steps that decrease the risk to one department without substantially increasing the cost to other departments.

Though it is appropriate for departments to operate autonomously in carrying out their primary function, decisions about ***information governance*** should be coordinated across all departments and stakeholders as they impact the

---

[11] *See* Appendix B for a discussion of the ***Information Governance*** Maturity Continuum.

organization as a whole. Because such decisions require an overall balancing between the needs and interests of different stakeholders, it is important for the ***information governance*** function to be independent within the organization. [12]

Principle 3. All *information* stakeholders should participate in an organization's *Information Governance* program.

Information Governance programs should seek to be inclusive and to involve all parts of an organization (business units, departments, etc.) that have an interest in the company's ***information***. [13] This may require involvement from all of the organization's departments or business units, which may require different levels and types of activity from stakeholders.

An inclusive process will ensure that decisions about ***information*** represent all viewpoints, identifying and resolving potential conflicts early and prior to any action being taken that could have an adverse impact to the organization. For example, an organization might consider a policy that bans MP3 (audio) files from being stored on company resources because they are often identified as unauthorized employee music collections, but there may be cases where such files contain training webcasts and may be needed by HR or corporate training. Without involvement of all parties, valuable ***information*** could be lost and adversely impact the organization. [14]

However, participation does not require a "seat at the table" for every person or even every department with an interest in the organization's ***information***. In larger organizations, active participation from every group could create an unwieldy team unable to reach decisions. A more effective approach would be to design an appropriate structure or methodology to ensure that all stakeholder interests are represented. An organization could create a process to identify groups with common interests, appoint certain committee members as proxies for other groups, or design surveys or feedback sessions to ensure that all interests are adequately identified and represented.

In most organizations, stakeholders from the core disciplines of records and ***information*** management, data privacy, ***information*** security, data ***governance*** and e-discovery should be represented in the ***Information Governance*** program. These disciplines will involve IT, Legal/Compliance, Risk, Audit and RIM functions. Representatives of lines of business and core operational functions should also be included to ensure that the practical needs of the organization are properly considered. It is important to include core operational functions that have unique ***information governance*** issues. For example, human resources and environmental functions typically have legally mandated retention for some of their ***information***.

Principle 4. The strategic objectives of an organization's *Information Governance* program should be based upon a comprehensive assessment of *information*-related practices, requirements, risks, and opportunities.

An effective ***Information Governance*** program should be designed, implemented, and monitored based upon organization-wide objectives established from a comprehensive assessment of the interests and concerns of key stakeholders within the organization, such as IT, Legal, Compliance, Records and ***Information*** Management, and various business units. The program objectives should address and coordinate the stakeholders' existing practices and approaches to issues such as records and ***information*** management, privacy and data security, and litigation preservation; and reconcile the practices and approaches with applicable legal requirements. Other major

---

[12] For further explanation, *see* Appendix B.

[13] *Cf.* The Sedona Conference, *Finding the Hidden ROI in* ***Information*** *Assets*, February 2011, *https://thesedonaconference.org/download-pub/466*.

[14] *Equal Employment Opportunity Commission v. Ventura Corp. LTD., Civ. No. 11-1700, 2013 WL 550550* (D.P.R. Feb. 12, 2013) (finding that even though there was no evidence of bad faith, a company that failed to preserve pertinent emails and hiring-related documents when it migrated to a new software system and restructured its office, ignored repeated requests to preserve the documents, and retained relevant email, that highlighted its missteps in preserving evidence amounted to spoliation that permitted sanction, exclusion of evidence, and an adverse inference instruction).

responsibilities of the ***Information Governance*** program should include gathering stakeholder requirements, such as those needed to create and publish requirements. Although the ***Information Governance*** program does not own the requirements, it owns responsibility for collecting requirements and considering them to arrive at a decision for the good of the organization overall.

To determine its ***information***-related practices, requirements, risks, and opportunities, an organization should first identify the various types of ***information*** in its possession, custody or control, assess whether it owns the ***information*** or possesses it for third-parties; and determine whether the ***information*** is held by the organization, by third-parties for the organization, or both. The organization should next identify its current ***information*** lifecycle practices, including practices pertaining to:

. Creation and/or receipt of ***information***;

. Determining location and media for storing ***information***, including in both active and inactive environments;

. Disaster recovery and business continuity;

. Security for private or confidential ***information***;

. Retention of ***information*** in both active and inactive environments;

. Implementation, maintenance and release of legal holds due to litigation or government proceedings; and

. Disposal/destruction of ***information***.

A review of existing written policies, procedures, retention schedules, data maps and contractual arrangements is helpful in identifying and understanding these ***information***-related practices. However, input from the organization's ***information*** stakeholders, including IT, Legal, Compliance, Records and ***Information*** Management, and business units, among others, is also essential to gaining an accurate and complete understanding of both the strengths of current ***information governance*** practices and areas where improvement may be necessary.

Organizations can then assess their identified ***information*** types and related practices in light of ***information*** opportunities, risks and compliance requirements including:

Opportunities

. Reducing costs and risks of complying with e-discovery obligations, by decreasing the volume of unnecessary ***information***, understanding where ***information*** is stored, and considering e-discovery costs and risks when approving locations or formats for creating or storing ***information***;

. Utilizing ***information*** to support evidence-based decision making;

. Optimizing accessibility of ***information*** to enhance productivity and efficiency;

. Realizing cost savings by decreasing the volume of unnecessary ***information***, and rationalizing storage options to better meet demands while reducing cost;

. Enabling access to ***information*** for new and valuable combinations and uses;

. Enhancing the organization's reputation as a trusted custodian of PHI, PIT, and other classes of protected ***information***; and

. Achieving cost savings and reducing risk through efficient and appropriately-scoped preservation of ***information*** for litigation or government proceedings.

Risks

. Loss of records or other valuable ***information***;

. Loss of integrity, authenticity, and reliability of records or other valuable ***information***;

. Unavailability of ***information*** vital to the organization's continued operation;

. Accumulation of ***information*** (both by the organization and third parties) not (i.e., never or no longer) required for legal compliance or business needs;

. Creation or storage of ***information*** in locations or formats that increase the risk or cost of e-discovery, without a corresponding business benefit to outweigh the increased risks and costs;

. Creation of internal RIM requirements that are not followed;

. Breach of PHI, PII, or other classes of protected ***information***;

. Harm to ***information*** from malicious access or attack;

. Inability or failure to detect and respond effectively to data breaches;

. Loss of intellectual property protection;

. Loss of privilege or confidentiality of ***information***;

. Failure to preserve ***information*** relevant to litigation or government proceedings;

. Over-preservation of ***information*** for litigation or government proceedings; and

. Failure to release ***information*** (held by the business, by the legal department, or by outside vendors like law firms, expert witnesses, review vendors, etc.), from preservation once no longer relevant to litigation or government proceedings.

Compliance Requirements

. Legal and contractual requirements for:

  . Records creation, retention, management, and disposition;

  . Privacy and security for PHI, PII, and other classes of protected ***information***;

  . Protection of intellectual property and confidential ***information***; and

  . Preserving ***information*** relevant to litigation or government proceedings.

These considerations will differ between jurisdictions, industry sectors, and organizations; and among organizations, there will be a range of risk tolerances and cultures regarding these matters. Industry standards, maturity models, and benchmarking data for comparable organizations are useful considerations for this assessment. [15]

---

[15] Useful standards and models include:

. International Organization for Standardization, ***Information*** *and Documentation-Management Systems for Records - Fundamentals and Vocabulary*, ISO 30300:2011 (2011).

. International Organization for Standardization, ***Information*** *and Documentation - Records Management - Parts 1 and 2*, ISO 15489-1:2001(2001); ISO 15489-2:2001 (2001).

. International Organization for Standardization, ***Information*** *Technology - Security Techniques*, ISO/IEC 27000:2012(2012); ISO/IEC 27010:2012 (2013); ISO/IEC TR 27019:2013 (2013).

An organization should use the results of the above assessment to determine its objectives for ***information governance***. Well-framed strategic objectives for ***information governance*** can guide the design and implementation of the organizations ***Information Governance*** program, helping to clarify what elements of structure, direction, resources, and accountability will be pursued, as discussed under Principle 5. Establishing strategic objectives in this manner should clarify decision making on priorities and funding of the effort. Strategic objectives should be measurable to better ensure that progress toward them can be observed and reported. Such measures may be quantitative (i.e., data volumes or run-rates) or qualitative (i.e., assessment or audit against program standards or upon completion of transactions or litigation matters). Measurability of objectives is essential for accountability, discussed under Principle 5. Perhaps the most important feature of this exercise is that it compels organizations to look beyond the confines of traditional silos within organizations. [16]

Principle 5. An *Information Governance* program should be established with the structure, direction, resources, and accountability to provide reasonable assurance that the program's objectives will be achieved.

To provide reasonable assurance that an ***Information Governance*** program will meet an organization's strategic objectives, the program should have structure, direction, resources, and accountability. Depending on the size of the organization, responsibilities such as change management and communication to raise awareness of the

---

. ARMA, *Generally Accepted Recordkeeping Principles(R) & **Information Governance** Maturity Model*, http://www.arma.org/r2/generally-accepted-br-recordkeeping-principles (2013).

. COBIT 5, *A Business Framework for the **Governance** and Management of Enterprise IT* (2012), *available at* http://www.isaca.org/COBIT/Pages/default.aspx.

. The Sedona Conference, *The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production* (Second Edition) (June 2007), https://thesedonaconference.org/download-pub/81.

. ISO standards, such as the ISO 30300 Series, *Management Systems for Records*; ISO 15489, Records Management; and the ISO 27000 Series, Code of Practice for ***Information*** Security Management.

. ARMA's *Generally Accepted Recordkeeping Principles(R) & **Information Governance** Maturity Model*,

. COBIT 5, *A Business Framework for the **Governance** and Management of Enterprise IT*.

[16] For example, in its ***information governance*** assessment, a financial services organization confirms that it has customer ***information*** subject to privacy and data security requirements, which it regularly transfers to the custody of various service providers in the ordinary operation of its business. From the siloed perspective of privacy and data security compliance, the organization satisfies the applicable requirements of the Federal Trade Commission's Safeguards Rule (FTC Standards for Safeguarding Customer ***Information***, 16 C.F.R. Pan 314 (2002)) by, *inter alia*, establishing internal controls for selecting and retaining service providers and by contractually requiring them to establish safeguards to ensure security for protected customer ***information***. The organization also periodically audits its service providers to assess the effectiveness of their ***information*** security safeguards.

However, through its ***information governance*** assessment, the organization determines that its internal requirements for records retention periods are not followed by its service providers, such that some service providers retain customer ***information*** for either a shorter or longer period of time than is required under the organization's records retention schedule. The organization also determines that its legal hold process may not include certain customer ***information*** relevant to litigation that is in the custody of various service providers, yet arguably within the "control" of the organization for discovery purposes.

As a result of the assessment, the organization decides that one of its strategic objectives will be to apply ***information governance*** controls to customer ***information*** possessed by its service providers. This strategic objective will allow the organization to ensure that service providers implement appropriate safeguards to protect customer ***information***, comply with the organization's records retention schedule and be responsive to legal holds that may be imposed upon customer ***information*** possessed by service providers.

information governance function, user training, creating the ***information governance*** matrix, and gathering metrics required for management control and monitoring may also be important.

Structure

One means of ensuring that an organization's various ***information*** needs are comprehensively addressed is to establish a unified framework in which the organization's various ***information*** types can be categorized according to ***information***-related compliance requirements and risk controls. Such a framework should categorize ***information*** types by content and context. [17] This will normally require input from a wide range of subject matter experts, including, for example, human resources, accounting, compliance, and environmental.

Attached to this framework of ***information*** types are the applicable rules the organization applies to the respective ***information***. These rules reflect legal and regulatory requirements for records retention, ***information*** management, and ***information*** security and protection. The rules reflect the organization's operational needs for how ***information*** will be retained, managed, and protected, and also the organization's risk controls. The unified framework allows the organization to identify, understand, and follow the appropriate rules for its ***information*** types.

In place of siloed structures governing data security, retention, and preservation, an organization could establish an ***information governance*** matrix. An ***information governance*** matrix is a classification structure for the organization's ***information*** types similar to a traditional records retention schedule or data security grid but which integrates all established rules governing the organization's ***information*** types. An ***information governance*** matrix is thus a repository of integrated rules for ***information*** from the organization's perspective as a whole, rather than merely one or more of its siloed functions. An ***information governance*** matrix should be designed to meet the needs of various audiences and multiple uses within the organization. It is essential, for all of the Company's business ***information***, that the Company establish and clearly communicate responsibility for complying with the integrated rules included in this ***governance*** matrix. Otherwise, "orphan data" can greatly increase the cost and risk of e-discovery.

An organization should strive to establish a common vocabulary for its various ***information*** types. [18] A common vocabulary helps ensure ***information*** is properly classified, so that the applicable rules for such ***information*** types can be identified and followed.

Direction

---

[17] ***Information*** context is significant, because different copies or instances of the same ***information*** content may be used for different purposes, thereby triggering different compliance requirements and risks. For example, a single contract may simultaneously exist in multiple instances for different purposes, including the original executed hard copy version; the scanned, digitized version that the organization declares as the official record of the contract; disaster recovery backup copies of the digitized contract; reference copies of the contract used for business convenience in various departments; and a preserved version of the contract under legal hold due to pending litigation. In each of these contexts, different compliance requirements and risks apply to the same ***information*** content of the contract.

[18] Whether an organization relics upon traditional structures such as records retention schedules and data security grids or integrates them into an ***information governance*** matrix, such structures are commonly organized as taxonomies. A taxonomy is a defined hierarchy with classes and sub-classes forming "trees" of classification. In a taxonomy, it is only possible to move downward into sub-classes, or upward into super classes that subsume all of the classes below. Taxonomies are flat and linear, and therefore limiting. In contrast, ontologies link classes in a non-hierarchical way, forming associations that are non-linear. Thus, the widget purchase order may be associated hierarchically with accounting recordkeeping; but at the same time, it may also be associated with documentation of contract rights and duties, and yet other business functions. Instances of the widget purchase order ***information*** may also, simultaneously, be associated with disaster recovery restoration, with ***information*** protection issues (due to where versions of the purchase order are located physically or virtually), and with applicable legal olds. The complexity of the digital environment, in which the same ***information*** content simultaneously exists in different locations and contexts, triggering different ***information governance*** rules, makes ontology a promising perspective for applying ***information governance*** to an organization's ***information***.

Organizations should communicate to all ***information*** users the organization's expectations for ***information governance***. Vehicles commonly used by organizations to provide such direction include policies, contracts, retention schedules or ***information governance*** matrices, procedures and protocols, and guidance and training.

Many organizations have an array of policies that directly or indirectly address ***information governance*** topics. Examples include a records-and-***information*** management policy, a communications policy, a computer use policy, an Internet and social media policy, a bring-your-own-device policy, an ***information*** security policy, and a legal hold policy. In many organizations, such ***information***-related policies accrete over time, each designed to meet the needs of discrete stakeholders and silos of the organization. They commonly address only limited aspects of ***information governance*** and may be in conflict with each other. Organizations should identify all such existing policies, review them for inconsistencies and gaps in coverage, and reconcile them or integrate the majority of these policies into a single ***information governance*** policy. Similar to the ***information governance*** matrix, an ***information governance*** policy expresses in one place all of the organization's policy-level expectations for ***governance*** of ***information***.

Contracts with third parties are another means of providing direction for ***information governance***. Organizations commonly allow ***information*** to be transferred to or held by third parties, such as service providers for business operations; management, legal, accounting, and technology consultants; data hosting providers; and hard-copy records storage providers. The organization's expectations for ***information governance*** should be communicated to such third parties through its contracts with them. [19] For example, engagement letters with law firms should confirm the firm's obligations to protect and preserve ***information***, and also the company's right to require destruction or return of ***information*** after the matter or engagement is concluded.

Organizations should also have specific procedures and protocols that provide explicit direction on ***information*** creation, receipt, use, dissemination, protection, retention, preservation, and ultimate disposition. Organizations should also establish effective guidance and training regarding ***information governance***, delivered in a way that empowers individuals to make timely, compliant decisions regarding ***information***. [20] Accordingly, training and guidance resources should be tailored to meet the specific needs of recipients and should provide the concrete direction the recipients need to make ***information***-related decisions consistent with the organization's ***information governance*** expectations.

Resources

Organizations should provide the people, technology, and implementation resources needed to support their ***Information Governance*** program and accomplish the organization's strategic objectives.

People resources include staffing of the management and administrative roles supporting the ***Information Governance*** program itself, as discussed above under Principle 3. Staffing should be commensurate with the program's scope and objectives, and roles and responsibilities should be defined. Key points of contact should be identified within the organization, and those in such roles should be accessible and responsive. People resources reflect the focus and engagement of stakeholder representatives, such as from Legal, IT, Compliance, Records and ***Information*** Management, other administrative functions, and lines of business. People resources also reflect the recognition that ***information governance*** is part of everyone's job responsibilities within the organization.

Technology resources include systems and applications used for creating, using, and storing ***information***, into which should be placed structures and controls for ***information governance***. Technology resources also include systems and applications for managing, tracking, and reporting regarding the ***Information Governance*** program

---

[19] In some regulated sectors, contractual control of ***information*** protection by such service providers is an explicit legal requirement. For example, HIPAA covered entities must contractually require their business associates to provide compliant security for electronic protected health ***information*** (ePHI) created, received, maintained, or transmitted on behalf of the covered entity. 45 C.F.R. § 164.314(a).

[20] *Day v. LSI Corp.*, No. CIV 11-186- TUC-CKJ, 2012 WL 6674434 (D. AZ. Dec. 20, 2012) (awarding sanctions for, among other things, failing to follow own document retention policy).

itself. Both kinds of technology should be used for the program's scope and objectives. ***Information governance*** technology resources should be procured only after requirements for such tools have been defined, consistent with the organization's strategic objectives for ***information governance***. Organizations should carefully consider whether the contemplated technology can fully achieve the program's desired objectives.

Implementation resources are also needed. These include project management tools and processes to be used as elements of the organizations ***Information Governance*** program.

Accountability

The effectiveness of an ***Information Governance*** program will turn upon whether the organization establishes accountability for meeting program expectations and for achieving the organization's strategic objectives for ***information governance***. In internal control systems, this atmosphere of accountability is the "control environment." [21] The organization's senior leadership establishes the "tone at the top" regarding strategic objectives, the importance of reaching these objectives, expected standards of conduct, and accountability. In all forms of direction, the visible commitment and support of the organization's senior leadership is crucial. [22]

Management reinforces these expectations, and the related roles, responsibilities, and accountability, across the organization. The ***Information Governance*** program should clarify roles and responsibilities, both for ***information*** users and also for those managing the ***Information Governance*** program.

Information Governance program objectives should be linked to observable and measurable outcomes; and compliance audits or comparable assessments of the program should be conducted on a regular, periodic basis, followed by appropriate corrective actions as needed. Program outcomes should be periodically compared to program objectives, and such outcomes should be tracked by those responsible for the ***Information Governance*** program.

The results of such outcome measures and program assessments should be reported periodically to the organization's senior leadership to provide reasonable assurance that the program's objectives are or will be satisfied.

Principle 6. The effective, timely, and consistent disposal of physical and electronic *information* that no longer needs to be retained should be a core component of any *Information Governance* program.

It is a sound strategic objective of a corporate organization to dispose [23] of ***information*** no longer required for compliance, legal hold purposes, or in the ordinary course of business. [24] If there is no legal retention obligation,

---

[21] The internal control concept of a control environment is a model that organizations may consider in pursuing ***information governance***, particularly for establishing accountability and managing risks around specific objectives. *See* Committee of Sponsoring Organizations of the Treadway Commission ("COSO"), *Internal Control-Integrated Framework Executive Summary - English*, (2013), http://www.coso.org/documents/Internal%20Control-Integrated%20Framework.pdf ("Internal control is a process effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.").

[22] In some aspects of ***information governance***, senior leadership involvement is legally required. For example, entities subject to the FTC's Red Flags Rule must obtain board-level approval of the initial Identity Theft Program, and must involve the board or senior management in the oversight, development, implementation, and administration of the Program. 16 C.F.R. § 681.1(e)(1) & (2). ISO 30300 provides that "Top management is responsible for setting an organization's direction and communicating priorities to employees and stakeholders."

[23] In this Commentary, the term "disposal" will be used narrowly to refer to the final destruction or deletion of ***information*** that no longer has any regulatory, statutory, compliance, legal or operational value and is not subject to any retention or preservation requirement. The effective disposal of data should purge all copies of that ***information*** from relevant systems so that they are no longer retrievable.

[24] *Managed Care Solutions, Inc. v. Essent Healthcare, 736 F. Supp.2d 1317, 1326* (S.D.Fla. Aug. 23, 2010) (rejecting the argument that there is no reasonable business routine demanding that data be destroyed after [13 months], especially in light of

information should be disposed as soon as the cost and risk of retaining the ***information*** is outweighed by the likely business value of retaining the ***information***. This may require a culture shift in some organizations that have developed a "keep it just in case" mentality. Typically, the business value decreases and the cost and risk increase as ***information*** ages. Timely disposal of ***information*** in a consistent and effective manner provides many benefits, including reduced storage and labor costs, [25] reduced costs and risks of complying with discovery obligations, and an increased ability to retrieve important organizational ***information***. Organizations should therefore consider procedures to achieve the regular destruction of unnecessary ***information***. [26] Organizations should also consider whether ***information*** considered private or confidential to third parties should be disposed of within a reasonable amount of time after it ceases to be useful to the organization in order to minimize the risk of disclosure.

While most organizations are familiar with managing paper records (and most retention schedules were drafted with paper in mind), it is important that the organization's retention schedules account for both hard copy and electronic records. For example, record owners may find it difficult to apply the concepts original versus copies to digital ***information***.

The term "hold" is used broadly in this commentary to cover preservation obligations that are independent from routine recordkeeping requirements, such as reasonably-anticipated or active litigation, governmental inquiries, outside audits, or contractual requirements. A hold may take the form of:

. A legal or litigation hold, i.e., the preservation of data for purposes of reasonably anticipated or active litigation or investigations;

. A tax hold, i.e., the preservation of ***information*** in ongoing audit or review of records related to tax obligations, such as financial and accounting records;

. A contractual hold is an agreed-upon obligation that an organization has with its customers, vendors, divested entities or other third parties that creates an obligation to preserve or dispose of ***information*** that exists separately from the retention schedule. [27]

Records Retention

To create a proper data disposal process, die organization should consider all applicable legal, regulatory, and contractual requirements, in conjunction with the business value of the organization's ***information***. The organization might begin this process by evaluating its legal/regulatory requirements at all levels and across all jurisdictions relevant to its business (state, federal and/or international) and clustering those records into categories. [28] This exercise will enable the organization to more easily identify the appropriate retention period

---

developments in the technology field (including the ability to inexpensively maintain documents at an off-site server) and industry standards stating the exact contrary." (citing *Matya v. Dexter Corp.*, No. 97-cv-763 C, 2006 WL 931870, at *11 (W.D. N.Y. Apr. 11, 2006) and *Floeter v. City of Orlando*, No. 6:05- CV-400-Orl-22KRS, 2007 WL 486633, at * 7 (M.D. Fla. Feb. 9, 2007)).

[25] Though some may view data storage as a low-cost concern, the maintenance, retention and discovery-based review of unnecessary ***information*** is far from cheap. In the aggregate, storage is quite expensive. *See, e.g.*, Jake Frazier, *'Hoarders': The Corporate Data Edition*, LAW TECHNOLOGY NEWS, (2012), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202581938140.

[26] Principle of Disposition, ARMA, *Generally Accepted Recordkeeping Principles(R)*, http://www.arma.org/r2/generally-accepted-br-recordkeeping-principles (last visited Dec.3, 2013) ("An organization shall provide secure and appropriate disposition for records and ***information*** that are no longer required to be maintained by applicable laws and the organizations policies.").

[27] An organization should be wary of this type of obligation, as it could create onerous obligations to dispose of copies of electronic data that may not be within the control of the organization, and inconsistent obligations where different contracts prescribe different retention periods.

[28] For some organizations, local, municipal and/or regional recordkeeping regulations may apply and, if so, should also be considered when developing an appropriate records retention schedule.

applicable to each category of records, while also facilitating the analysis of certain key factors relevant to the retention determination, including the cost vs. risk associated with a category of records. [29]

It is important for the organization to remember that the operational value of a records category cannot be the sole consideration in determining a proper retention schedule; legal, regulatory and compliance objectives are of paramount concern. It is equally important, however, that operational value (e.g., maintenance of historical records, research and development processes, other business-driven objectives) be considered as the organization formulates its retention protocols. Otherwise, the organization may squander valuable opportunities to reduce cost while minimizing risk. For example, organizations should strive to avoid retaining ***information*** simply because it may possibly be useful at some point in the future and instead undertake a cost-benefit and a risk-benefit analysis with respect to each category of data it maintains, thereby ensuring that the advantages of retaining a given set of ***information*** outweigh the potential costs and risks associated with disposing of that ***information***.

Hold/Preservation Analysis

Before the organization disposes of any business records, it should conduct a hold analysis to determine whether there are any legal/regulatory or other obligations in place that require the organization to retain ***information***, regardless of its business value. In order to effectively identify its preservation obligations, it is advisable for the organization to develop and implement protocols designed to track legal/regulatory holds and map them to the relevant sources of ***information***, or take other steps to label, segregate and preserve the ***information***. A key aspect of this exercise is to communicate those protocols to the relevant individuals within the organization, and provide a point of contact (typically, a member of the legal or compliance department) who will address any questions regarding hold procedures and best practices. [30]

It is important for the relevant constituencies within the organization -- not just the legal/compliance department -- to understand that a legal hold supersedes all other records and ***information*** management and retention schedules, and that a hold requires the immediate suspension of the disposal process for all affected ***information*** during the time mandated by the hold. Thus, it is critical for the organization to incorporate a "hold and release" capability into its records disposition process, so that once the hold is released or has expired, the affected ***information*** can be placed back into the appropriate retention schedule.

Disposition

Once the organization verifies that no legal, regulatory, or operational requirements apply to the ***information***, disposition decisions can be made. In some circumstances, an organization may be able to determine from readily available ***information*** whether a record retention or legal preservation requirement applies. In other circumstances, a more detailed investigation and analysis may be required. The analytical approach to such situations is beyond the scope of this Commentary and is discussed more fully in the Sedona publication entitled, "*The Sedona Conference Commentary on Inactive* ***Information*** *Sources*." [31]

Principle 7. When *information governance* decisions require an organization to reconcile conflicting laws or obligations, the organization should act in good faith and give due respect to considerations such as privacy, data protection, security, records and *information* management, risk management, and sound business practices.

---

[29] For more ***information***, *see* ARMA International Standards and Best Practices, *http://www.arma.org/r2/standards-amp-best-practices* (last visited Dec.3, 2013) as well as the ARMAs Generally Accepted Recordkeeping Principles: Principle or Disposition, *http://www.arma.org/r2/generally-accepted-br-recordkeeping-principles* (last visited Dec. 3, 2013).

[30] For further ***information*** on legal holds, *see The Sedona Conference Commentary on Legal Holds: The Trigger & The Process*, 11 SEDONA CONE J. 265 (2010), *https://thesedonaconference.org/download-pub/470*.

[31] *See, The Sedona Conference Commentary on Inactive* ***Information*** *Sources*, (2009) *https://thesedonaconferencc.org/download-pub/64*.

Organizations often confront conflicting laws or obligations that apply to the same ***information***, particularly when the organization conducts business across numerous jurisdictions. [32] A common example involves the tension between the European Union Data Protection Directive, which prohibits transferring "personal ***information***," and United States federal court jurisprudence that mandates the production of such ***information*** during the discovery process. [33] In other circumstances, an organization may be required to preserve certain ***information*** for a specified period of time, while another jurisdiction may require such ***information*** be destroyed upon the owner's request.

When faced with ***information governance*** decisions triggered by such conflicts, the organization's key objective should be good faith compliance with all laws and obligations. Due deference should be afforded to conflicting laws or obligations, particularly when the conflict arises out of interests that span different jurisdictions. [34] Further, the most significant legal/regulatory and business considerations should be prioritized; not all conflicts are capable of complete resolution, and the organization will ultimately need to balance the competing needs, demands, and viewpoints of the stakeholders involved. To the extent compliance with all laws and obligations is not possible or practical; the organization should thoroughly document its efforts to reconcile the conflict and its resulting decision-making process.

Principle 8. If an organization has acted in good faith in its attempt to reconcile conflicting laws and obligations, a court or other authority reviewing the organization's actions should do so under a standard of reasonableness according to the circumstances at the time such actions were taken.

An organization's actions may be subject to review by a court or other governing authority regarding its attempt at resolving conflicting laws and obligations. That review should consider the specific circumstances when the ***information governance*** decision under review was made. Any judgment of the correctness of past actions to resolve conflicts should be based solely upon what was known at the time the decisions were made. Where a party has acted in good faith, it would be patently unfair to consider what they might have known had they possessed superior prescience. [35]

---

[32] *Devon Robotics v. DeViedma*, Civil Action No. 09- *CV-3552 2010 WL 3985877* (E.D. Pa. Oct. 8, 2010). The plaintiff in a breach of fiduciary duty and tortious interference requested all ESI relating to the former employee defendant, his Italian employer (a rival), and the alleged breach of contract between the plaintiff and the defendants new employer. The defendant moved for a protective order regarding the production of "documents owned by his employer," arguing that the disclosure was prohibited by the Italian Personal Data Protection Code. The court found that the defendant did not show good cause for a protective order and denied the motion, writing that the defendant "made nothing but a blanket assertion that any disclosure could violate Italian law." The court also stressed the importance of the requested ESI to the plaintiffs claims and the comity factors outlined in *Societe Nationals (482 U.S. 522 (1987))* weighed in favor of disclosure.

[33] *See, e.g. Heraeus Kulzer, GmbH v. Biomet, Inc., 633 F.3d 591 (7th Cir. 2011).*

[34] For example, with respect to the transfer of ***information*** from France to the U.S. for use in legal proceedings, which allegedly would have violated a French blocking statute, the U.S. Supreme Court held that U.S. courts should "take care to demonstrate due respect for any special problem confronted by the foreign litigant on account of its nationality or the location of its operations, and for any sovereign interest expressed by a foreign state." *Société Nationale Industrielle Aérospatiale v. United States District Court for the Southern District of Iowa, 482 U.S. 522, 546 (1987).* In so doing, "the concept of international comity requires in this context a … particularized analysis of the respective interests of the foreign nation and the requesting nation." Id. at 543-44.

[35] *The Sedona Conference International Principles on Discovery, Disclosure & Data Protection*; Best Practices, Recommendations & Principles for Addressing the Preservation & Discovery or Protected Data in U.S. Litigation (European Union Edition), (2011), *https://thesedonaconference.org/download-pub/495*. Principle 2: "Where full compliance with both Data Protection Laws and preservation, disclosure, and discovery obligations presents a conflict, a party's conduct should be judged by a court or data protection authority under a standard of good faith and reasonableness."*See also*, ABA Resolution 103 (2012) (adopted), *http://www.americanbar.org/content/dam/aba/administrative/house_of_delegates/resolutions/2012_hod_midyear_meeting_103.doc*. 26k-2012-11-10: "t[T]he American Bar Association urges that, where possible in the context of the proceedings before them, U.S. federal, state, territorial, tribal and local courts consider and respect, as appropriate, the data protection and privacy laws of

Application of the reasonableness standards requires that a court or other authority objectively assess the organization's actions or decisions in comparison to the actions or decisions made by a hypothetical, similarly-situated organization acting reasonably under the same circumstances. In *Lewy v. Remington Arms Co., Inc., 836 F.2d 1104 (8th Cir. 1988),* the court outlined factors to be considered in assessing the reasonableness of a record retention policy for a spoliation instruction, including: (i) whether the policy was reasonable considering the facts and circumstances surrounding the relevant documents (i.e., whether a three year retention policy is reasonable for a class of materials, such as email); (ii) whether any lawsuits relating to the documents had been filed, or may have been expected; and (iii) whether the document retention policy was instituted in bad faith. Id. at 1112.

In determining good faith, courts or other authorities should give due deference to decisions by corporate officers or directors by applying the "business judgment rule," which is a presumption that a business decision was made "on an informed basis, in good faith and in the honest belief that the action taken was in the best interests of the company." *Aronson v. Lewis, 473 A.2d 805, 812 (Del. 1984)* (citations omitted).

Principle 9. An organization should consider reasonable measures to maintain the integrity and availability of long-term *information* assets throughout their intended useful life.

If the intended useful life of an ***information*** asset is long enough that risks or concerns may arise regarding the ongoing integrity and availability of the ***information***, then organizations should consider appropriate measures designed to protect those ***information*** assets. Therefore, *long-term* planning for availability and integrity depends on the circumstances involved, including the asset's purpose and storage media options.

For example, if your intended retention period is 25 years and the media format you will be using has an expected life of 12 years, then specific planning will be required to ensure the ongoing integrity and availability of that ***information***. Failing to ensure the integrity and availability of ***information*** assets may bring the risk of sanctions if an organization is unable to fulfill e-discovery obligations. [36]

This principle is limited to "systems of record", meaning that copies (such as convenience copies) are outside its scope. Backup and recovery, disaster recovery, and redundant storage paradigms such as 'RAID' are well-understood disciplines dictated by operational business continuity requirements and are therefore not covered by this Commentary. Logical defects prior to "long-term" storage also are not covered by this principle or Commentary.

Long Term Digital Assets

The phrase "long-term" is used to mean a time-frame sufficiently long to involve planning for concerns such as the physical degradation of the storage medium or the impact of changing technologies.

Planning for the ongoing integrity and availability of long-term ***information*** assets is important for both physical and digital ***information***, but it is important for digital assets that may have a long lifecycle or retention period. The risks and considerations should be evaluated as part of the long-term retention strategy.

To maximize the probability of ensuring the ongoing integrity and availability of digital assets throughout their intended useful life, organizations should make a good-faith attempt to balance risk and cost. Creating a long-term retention strategy appropriate to the value and type of the ***information*** involves considering a broad range of factors pertaining to the digital assets and the circumstances of the organization itself. These factors should include business value, regulatory importance, intended retention schedule, legal hold status, file format, continued availability of the technologies required to access and read, the likely failure rate of the storage medium as it is configured, the available budget and resources of the organization, and/or (for 3rd party services such as *cloud* storage, SaaS, etc.), the contractual agreements between the customer and provider. [37]

---

any applicable foreign sovereign, and the interests of any person who is subject to or benefits from such laws, with regard to data sought in discovery in civil litigation."

[36] *United States v. Universal Health Servs., Inc.*, No. 1:07cv000054, 2011 WL 3426046 (W.D. Va. Aug. 5, 2011).

[37] For a more detailed explanation of the specific areas of risk for digital assets, *see* Appendix C.

Principle 10. An organization should consider leveraging the power of new technologies in its *Information Governance* program.

For many organizations, reliance on end-users to effectively manage ***information*** continues to work well. These organizations should consider how technology can help individuals to better manage the ***information*** that they are responsible for, and to monitor management of the ***information***. Examples of the former include limitations on the size of email accounts, or systems that automatically delete emails unless they are moved from the inbox or sent box. Appropriate use of this technology can significantly decrease the cost and risk of e-discovery because emails frequently make up a significant percentage of ***information*** that is collected for litigation or government investigations. Similarly, organizations should consider using technology that automatically deletes voicemails after a fixed number of days. Companies can also monitor for over-retention by providing management with lists of the largest email accounts or reports on data that has not been accessed recently.

However, organizations should consider using advanced tools and technologies to perform various types of categorization and classification activities. While the rapid advances in technology threaten to render obsolete the technology described in this commentary, an organization should consider using technologies such as machine learning, auto-categorization, and predictive analytics to perform multiple purposes, including: (i) optimizing the ***governance*** of ***information*** for traditional RIM; (ii) providing more efficient and more efficacious means of accessing ***information*** for e-discovery, compliance, and open records laws; and (iii) advancing sophisticated business intelligence across the enterprise.

Machine Learning, Auto-Categorization, and Predictive Analytics Defined

Machine learning is the "[f]ield of study that gives computers the ability to learn without being explicitly programmed." [38] Training filters to recognize spam email is one common example of machine learning. In theory, just about any classification problem arising in ***information governance*** can benefit from being modeled by machine learning techniques. Some of these techniques do not rely on human intervention: for example, clustering or auto categorizing data into data types or classifications can be accomplished through software alone analyzing the properties of a data set.

One machine learning technique of particular utility involves active learning by software through human interaction on the front end, where humans train the systems to learn through examples. "Predictive coding" and "technology-assisted review" are terms used in the e-discovery arena that rely on humans coding seed sets of data into responsive and nonresponsive categories, with software then analyzing the remaining huge repositories of data. [39] As used here, "predictive analytics" means any machine learning technique that combines human intervention on the front end with the power of machine learning, to optimize the classification of ***information*** through automated rules.

New Technologies Meet Traditional RIM

If the structure or volume of ***information*** flowing through networks does not allow continued reliance on "end-users" to categorize content, organizations should consider taking steps that shift the burden of traditional records and ***information*** management from individuals to technology through auto-categorization of content. Organizations should, therefore, consider taking steps that shift the burden of traditional records and ***information*** management from individuals to technology through auto-categorization of content. For example, organizations may use existing software to analyze and categorize the contents of email for purposes of defensible deletion of transitory, non-

---

[38] Arthur L. Samuel, "*Studies in Machine Learning Using the Game of Checkers*," IBM JOURNAL OF RESEARCH AND DEVELOPMENT 3(3):211-229 (1959).

[39] *See generally*, The Grossman-Cormack Glossary of Technology Assisted Review, 7 FED. CTS. L. REV. 1 (2013).

substantive or non-record content. [40] Organizations increasingly utilize predictive analytics to assist in categorization functions, where individuals train software to differentiate between types of records.

For e-discovery, the first judicial opinions approving the use of predictive coding and technology-assisted review techniques for document review in e-discovery were published in 2012. [41] In one case, the court stated that "the Bar should take away from this Opinion … that computer-assisted review is an available tool and should be seriously considered for use in large-data-volume cases where it may save the producing party (or both parties) significant amounts of legal fees in document review." [42] An important study by the Rand Corporation, anticipating this new direction in the law, concluded that predictive coding may significantly reduce e-discovery costs by reducing the number of documents requiring eyes-on review. [43]

Predictive Analytics and Compliance

Predictive analytics is also increasingly being utilized by organizations outside of the e-discovery context, including in investigations and as an element of compliance programs. Predictive analytics is being used in compliance programs to predict and prevent wrongful or negligent conduct that might result in data breach or loss. Similar to how this technology is being used in litigation and investigations, predictive analytics is being used as an early warning system. To this end, companies use exemplar documents, sometimes in conjunction with search terms, to periodically search a target corpus of documents, usually email, to detect improper conduct.

Predictive Analytics and Business Intelligence

At its most fundamental level, predictive analytics assists in identifying ***information*** that may help to answer a question. There is no limit to the questions predictive analytics can help answer. Companies are beginning to use predictive analytics to develop business intelligence about the company, its ***information*** assets, and the market in which it operates.

Principle 11. An organization should periodically review and update its *Information Governance* program to ensure that it continues to meet the organization's needs as they evolve.

Organizations and their environments change. The footprint and nature of the organization's operations may expand, contract, or transform, and its technology capabilities and uses will evolve. The organization's environment will also change, including legal requirements for the retention, protection, preservation, and disposal of ***information***. And new ***information***-related risks will also arise as time passes. Review of at least some aspects of many organizations' ***Information Governance*** programs is legally required, [44] and regardless, is prudent given

---

[40] The National Archives and Records Administration has endorsed the use of email archiving and capture technologies using smart filters to sort content through role-based and rule-based architectures. *See* NARA Bulletin 2013-02, *Guidance on a New Approach to Managing Email Records*, (Aug. 29, 2013), *http://www.archives.gov/records-mgmt/bulletins/2013/2013-02.html*.

[41] *See, e.g., Da Silva Moore v. Publicis Groupe, 287 F.R.D. 182 (S.D.N.Y. 2012), approved and adopted in Da Silva Moore v. Publicis Groupe*, No. 11 Civ. 1279(ALC)(AJP), *2012 WL 1446534* (S.D.N.Y. Apr. 26, 2012); Global Aerospace Inc., et al. v. Landow Aviation, L.P., et al, No. CL 61040, 2012 WL 1431215 (Va. Cir. Ct. Apr. 23, 2012); *In re Actos (Pioglitazone) Products*, No. 6-11-md-2299, *2012 WL 3899669* (W.D. La. July 27, 2012).

[42] *Da Silva Moore, 287 F.R.D. at 193.*

[43] N. Pace & L. Zakaras, "*Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery*," RAND Report (2012), *http://www.rand.org/pubs/monographs/MG1208.html*.

[44] For example, HIPAA policies and procedures must Be reviewed periodically and updated as needed in response to environmental or operational changes affecting the security of electronic protected health ***information***. 45 C.F.R. § 164.316(b)(2)(iii). HIPAA security measures must also be reviewed and modified as needed to continue providing reasonable and appropriate protection for ePHI. 45 C.F.R. § 164.306(e). Comprehensive ***information*** security programs for customer ***information*** under the Gramm-Leach-Bliley Act must be evaluated and adjusted in light of any material changes in operations or business arrangements. 16 C.F.R. § 314.4(e). Entities subject to the FTC's Red Flags Rule must ensure that their mandated

the inevitability of organizational and environmental change. Organizations, therefore, should periodically review and update their ***Information Governance*** program.

Program review differs from the monitoring activities that should be embedded in the organization's ***Information Governance*** program. Such monitoring activities observe whether ***information***-related practices comply with the program's rules and risk controls. *See* Principle 5, Accountability. The program review should seek to determine whether the program itself, and its rules and risk controls, remain appropriate for governing the organization's ***information*** in light of organizational and environmental changes. A flawlessly-executed ***Information Governance*** program will still result in compliance and risk exposures if elements of the program have become obsolete due to changed circumstances.

The review of the ***Information Governance*** program is akin to the assessment described under Principle 4. The organization should:

. identify any significant changes in its life cycle practices for ***information***;

. identify significant changes in applicable compliance requirements and risks regarding its ***information***;

. review the organization's strategic objectives for ***information governance*** in light of internal or external changes; and

. review the results from monitoring and measuring performance of the organization's ***Information Governance*** program, as an indicator of whether the program's rules and risk controls are adequate or should be refined.

Those responsible for administering the organization's ***Information Governance*** program should be involved in the program review. The need for objectivity in conducting such a review may make it valuable to have an independent review of the program. And ultimately, because senior leadership is responsible for the results of ***information governance*** at the organization, such senior leadership should participate appropriately in the review process, receive the results of the review, and then provide direction, support, and resources for needed changes in the program.

No bright-line rule governs how frequently an ***Information Governance*** program should be reviewed. As with other business-driven initiatives, the frequency of review will most likely depend on many factors relating to the organization. [45] If an organization is rapidly changing through frequent acquisitions and divestitures, or periodically undergoes major updates to its technology systems, then its ***information*** environment is likely to be ever-changing to adapt to its new structure or systems. Alternatively, if an organization is relatively mature, has a stable operations model, or is not governed by frequently changing governmental regulations, it may be reasonable for it to conduct its reviews less frequently (i.e., biannually), to reassess and identify potential modifications to its recordkeeping, data security, and operational requirements. Further, an organization may be subject to external pressures, such as regulations subject to frequent modification or regular compliance audits that require systemic changes; in such cases, the organization should be prepared to review and revise its ***information governance*** policies on an ongoing basis to meet the challenges posed by such changes. An organization should track pending legislation and regulations relevant to its industry to facilitate continued compliance with the regulations that affect its operations. It

---

Identity Theft Program is updated periodically to reflect changes in risks to customers or to their safety and soundness regarding identity theft. 16 C.F.R. § 681.1(d)(2)(iii). And entities that own or license personal ***information*** about Massachusetts' residents must review their ***information*** security measures at least annually or whenever a material change in business practices reasonably implicates the security or integrity of records containing such personal ***information***. 201 CMR. 17.03(2)(i).

[45] Determining the appropriate frequency of review is a matter of business judgment. Courts generally defer to decisions by corporate officers and directors pursuant to the "business judgment rule," which is built upon the presumption that business decisions are made "on an informed basis, in good faith and in the honest belief that the action taken was in the best interests of the company." *Aronson v. Lewis, 473 A.2d 805, 812 (Del. 1984), (overruled on other grounds by Brehm v. Eisner, 746 A.2d 244 (Del. 2000).*

would be prudent to include a review of its ***information governance*** policies and procedures as part of its response to such developments.

Because of the ongoing program review, update, and execution, an organization will have reasonable assurance its ***Information Governance*** program continues to meet both legal requirements and also the organization's strategic objectives for ***information***.

APPENDIX A

Intersections

Intersections Create Opportunities and Challenges

Although the functional areas of RIM, E-Discovery, Privacy and ***Information*** Security are frequently separate, a successful ***Information Governance*** program requires them to work together. As there is some natural overlap between the three groups, some of this will come naturally and provides opportunities to combine resources and budgets. Conversely, in some areas the goals of intersecting groups may clash and require resolution before an initiative can move forward. Identifying and leveraging these areas early in a program is an important task. The table below defines many of the synergies and conflicts in the intersections of these groups.

Functional Area Focus	**RIM** **Intersection with** **Functional Area**
RIM Primary Focus: RIM programs ensure that records and ***information*** are properly maintained, accessed, and ultimately disposed of in accordance with statutory and regulatory requirements and with consumer expectations. They also ensure that those organizations with which there is a third-party relationship endorse the same safeguards and have appropriate means of guaranteeing compliance.	N/A

Functional Area Focus	RIM Intersection with Functional Area

Functional Area Focus	E-Discovery Intersection with Fuctional Area
RIM Primary Focus: RIM programs ensure that records and ***information*** are properly maintained, accessed, and ultimately disposed of in accordance with statutory and regulatory requirements and with consumer expectations. They also ensure that those organizations with which there is a third-party relationship endorse the same safeguards and have appropriate means of guaranteeing compliance.	Potential Synergy: . Similar metadata concerns. . Work together to respond to document requests by locating and preserving relevant ***information***. . Support consistent defensible disposition of ***information*** in accordance with an organization's legal, regulatory and operational requirements. . Enables organization to know what they have and identify, preserve, retrieve, search, produce and appropriately destroy in normal course of business. . RIM protects against loss of content that could lead to sanctions, financial loss and brand risk during e-discovery. . RIM serves as evidence of official policy and helps ensure that evidence can be authenticated.

Functional Area Focus	E-Discovery Intersection with Fuctional Area
	Potential Friction: . Could be responsible for retention of drafts or outdated content due to relevancy. . RIM focus is can be more narrowly targeted to "records" while e-discovery is broadly on ESI

Functional Area Focus	Privacy Intersection with Fuctional Area
RIM Primary Focus: RIM programs ensure that records and ***information*** are properly maintained, accessed, and ultimately disposed of in accordance with statutory and regulatory requirements and with consumer expectations. They also ensure that those organizations with which there is a third-party relationship endorse the same safeguards and have appropriate means of guaranteeing compliance.	Potential Synergy: . Defines requirements for identification and classification of sensitive ***information***. Potential Friction: . RIM may need wide access and distribution while Privacy seeks limits.

Functional Area Focus	Privacy Intersection with Fuctional Area

Functional Area Focus	Security Intersection with Fuctional Area
RIM Primary Focus: RIM programs ensure that records and ***information*** are properly maintained, accessed, and ultimately disposed of in accordance with statutory and regulatory requirements and with consumer expectations. They also ensure that those organizations with which there is a third-party relationship endorse the same safeguards and have appropriate means of guaranteeing compliance.	Potential Synergy: . Ensures that sensitive ***information*** is properly maintained, identified and content is classified. . Ensures that sensitive data and ***information*** is properly maintained, accessed and disposed of according to legal and regulatory requirements. Potential Friction: . RIM may need wide access and distribution while Security seeks limits. . Encryption may be

Functional Area Focus	Security Intersection with Fuctional Area
	required in Security but frustrate accessibility by RIM.

Functional Area Focus	RIM Intersection with Functional Area
E-Discovery Primary Focus: Preservation of electronically stored ***information*** that is potentially relevant to impending or ongoing litigation and is processed in a timely, auditable and efficient manner.	See RIM / E-Discovery intersection above

Functional Area Focus	E-Discovery

	Intersection with Fuctional Area
E-Discovery Primary Focus: Preservation of electronically stored ***information*** that is potentially relevant to impending or ongoing litigation and is processed in a timely, auditable and efficient manner.	N/A

Functional Area Focus	Privacy Intersection with Fuctional Area
E-Discovery Primary Focus: Preservation of electronically stored ***information*** that is potentially relevant to impending or ongoing litigation and is processed in a timely, auditable and efficient manner.	Potential Synergy: . Identification at point of creation of ***information*** subject to privacy regulations may reduce risk that private ***information*** will be produced. Potential Friction: . Producing private ***information*** protected by another country's laws can

Functional Area Focus	Intersection with Fuctional Area
	Privacy result in criminal or civil sanctions. . Refusing to preserve and produce private ***information*** may result in civil or criminal penalties under US Law.
Functional Area Focus	Intersection with Fuctional Area
E-Discovery Primary Focus: Preservation of electronically stored ***information*** that is potentially relevant to impending or ongoing litigation and is processed in a timely, auditable and efficient manner.	Security Potential Synergy: . Ensures that sensitive data and ***information*** is available, if relevant; and that out-of-date ***information*** is disposed of according to legal and regulatory requirements. . Satisfies an organization's "duty to preserve" for forensic collections. Potential Friction: . Security encryption requirements can hamper e-discovery efforts.
Functional Area Focus	Intersection with Functional Area
	RIM

Functional Area Focus	RIM
Security Primary Focus: Ensuring the confidentiality, integrity, and availability of ***information*** and assets.	See RIM/Security intersection above

Functional Area Focus	E-Discovery Intersection with Fuctional Area
Security Primary Focus: Ensuring the confidentiality, integrity, and availability of ***information*** and assets.	Potential Synergy: . Ensures that sensitive data and ***information*** is available, if relevant, and that out-of-date ***information*** is disposed of according to legal and regulatory requirements. . Satisfies an organization's "duty to preserve" for forensic collections. Potential Friction: . Security encryption requirements can

Functional Area Focus	Privacy Intersection with Fuctional Area
Security Primary Focus: Ensuring the confidentiality, integrity, and availability of ***information*** and assets.	Potential Synergy: . Security enforces the access rights defined by privacy. Potential Friction: . Privacy requirements may hamper security investigations

Functional Area Focus	Security Intersection with Fuctional Area
Security	N/A

Functional Area Focus	Security
Primary Focus: Ensuring the confidentiality, integrity, and availability of ***information*** and assets.	

APPENDIX B

Maturity Continuum as it Relates to Independence

It is important to consider the independence of the ***Information Governance*** function of an organization when making determinations such as assessing the current maturity, or planning how to increase the future maturity of an ***Information Governance*** program.

While not all organizations have a sufficiently mature ***Information Governance*** program to warrant the appointment of a C level executive in this role, we believe that organizations must ultimately view ***information governance*** as requiring an executive leader that is accountable to the CEO or COO in order to ensure that decisions are made in the best interests of the overall organization, rather than for the good of discrete departments.

A common difficulty when balancing costs and risks occurs when the choices have dissimilar characteristics that make comparison difficult. For example, a clearly-defined cost saving may need to be weighed against a high impact, low-probability event, such as statutory fines in the event of leakage of protected data, where it is difficult to quantify the probability of the event occurring or the costs. Whatever risk management methodology is used to balance cost and risk, it will be more accurate to make the determination by looking at the problem from the perspective of the overall organizational impact.

However, if the executive in charge of ***information governance*** reports to an individual department, there is the potential for the interests of that department to be given greater weight than the overall interests of the organization. The simple fact that the department to which the executive reports funds their work and rates their job performance may result in such a bias.

Therefore, the level of independence of the ***information governance*** function of an organization is an important component of the ***information governance*** maturity continuum.

Maturity and Independence

The following discussion is intended as a reference to aid in assessing the current level of maturity of an ***information*** function, planning how to move an organization further along the ***information governance*** maturity continuum, or making a determination as to what is *sufficient* independence for a given organization. The concepts described below can be adapted for the specific circumstances of an organization.

Note: The following graphics are highly simplified, generic representations of potential organizational structures at varying points along the maturity continuum. The graphics depict the coordination and accountability at a departmental level. Specific functions such as RIM, Privacy, ***Information*** Security, E-Discovery, etc. are intentionally not shown because they generally reside within a stakeholder department.

Immature

Immaturity is characterized by a lack of over-arching coordination of ***information governance*** stakeholders and no single point of accountability to the CEO or COO for overall ***governance*** of ***information***.

At the immature end of the maturity continuum, lack of coordination creates a potential for important requirements being missed. Decisions and requirements reside in silos, and cross-functional coordination is ad hoc. There is a potential for departmental decisions that conflict with other stakeholder requirements and which are not in the interests of the organization overall. There is also a potential for inconsistent treatment of different items in the same category in the same circumstances.

Less Mature

At this area of the maturity continuum, ownership of ***information governance*** process resides within a stakeholder department.

There is a potential conflict of interest since ownership must reside in a stakeholder department, which presents the problem of misaligned incentives.

More Mature

At this area of the maturity continuum, ownership of ***Information Governance*** process resides in a stakeholder department but is accountable to a steering committee of *C* level executives from the stakeholder departments who are accountable to the CEO or COO.

There is still a potential for conflict of interest for the executive in charge of ***Information Governance*** (who resides in a stakeholder department) and for the *C* level executives on the ***Information Governance*** steering committee because the goals of the individual departments may conflict with the goals of the overall ***Information Governance*** program.

Mature

A mature Independence ***Governance*** function is characterized by an executive who resides in a separate ***Information Governance*** department who is accountable to the CEO or COO for coordinating stakeholders across all departments and functions and balancing decisions for the benefit of the organization overall.

Appendix C

Risks Associated with Digital Assets

Risks

There are specific areas of risk for digital assets that organizations should consider, including:

Integrity

The term "integrity" is used to mean the authenticity and reliability of the ***information***. In some situations this may simply mean the logical content of the ***information*** has not been altered. In other situations it may mean the file can be guaranteed not to have changed.

The integrity of the ***information***, or of ***information*** required to access the ***information*** (such as an index or necessary metadata) may be compromised by factors such as unauthorized alteration, or degradation of the storage medium. These risks can become particularly acute during platform migration.

Consideration should be given to: (a) the level of integrity required both for the digital asset in question and the technologies required to read and access the data, and (b) the level of difficulty involved in repairing or recovering damaged digital ***information***.

Careful consideration should be given to the file format, storage medium (including the configuration of that storage medium), and the circumstances of operation and storage, in order to ascertain the likelihood of data loss.

Digital storage media without moving parts such as flash drives, solid state drives, and tape, or with rarely moving parts (such as storage devices intended for infrequent use that power off" when not in use) still fail. Unused storage media on a shelf (for example, forensic collections on individual storage media in an evidence lab) will eventually become unusable. Given the relatively short lifespan (say, three-to-five years) of some items of storage media, a legal hold or retention requirement that may potentially exceed the reasonably expected lifespan could necessitate specific *long-term* planning due to the failure rate of the technology involved.

Availability

The term "availability" is used to mean "able to be used when needed," which includes:

. any element (such as security mechanisms to protect the data, access rights required to access the data, or applications required to interpret or read the data);

. being able to access ***information*** in a timely manner (for example within applicable service-level agreements, contractual requirements, or timeframes indicated by legal requirements);

. being available within a pre-agreed lead-time (depending on business need -- for example, a week).

Note that availability does not necessarily mean continuous availability.

The availability of ***information***, or ***information*** required to access the ***information*** (such as an index or necessary metadata) may be compromised by obsolescence or unavailability of technology required for accessing the ***information*** (or index, or necessary metadata) in a timely manner.

Considerations

When planning for ongoing integrity and availability of digital assets throughout their intended useful life, important considerations include:

Technology Refresh Period

[SEE FIGURE IN ORIGINAL]

The phrase "technology refresh period" is used to refer to the timeframe in which technology components are expected to fail, and within which planning needs to occur for replacing those components.

Organizations should exercise prudence when considering the technology refresh period for long-term digital assets. For example, if the expected lifespan of the storage medium is seven years, then the technology refresh period should be less than seven years. The timing of the technology refresh period compared to the technology's expected lifespan is a matter of risk calibration and business judgment.

Planned Migrations

Obsolescence of technology is a major consideration in long-term storage of digital assets and requires careful planning. Migrations (moving to a new platform for the archive as a whole or for a component of the archive) are a consequence of obsolescence that must be planned. All elements of the archiving system including search-and-retrieval capability as well as storage medium should be considered in terms of obsolescence. Organizations should consider creating an obsolescence review period as part of their long-term archival planning, because unlike a technology refresh period (which can be ascertained in advance for each technology refresh cycle by reference to the expected life of the technology components) the probable time of obsolescence may not be knowable in advance.

Migrations may also require format conversions, and integrity-checking technologies (see below) are particularly critical to ensure the data is not inadvertently changed during a migration.

Matching Storage Medium to the type of Electronic ***Information***

It is important to match the characteristics of the storage medium to the requirements of the ***information*** being stored. For example, micrographics work particularly well for text documents -- particularly text documents held for reference purposes -- but not for binary files such as audio files or CAD (Computer Aided Design) files. Micrographics also may not work well for files that need to be in digital format when used because a scanning or conversion process will be required before the file can be used.

The expected failure rate of the storage medium should be considered in terms of the expected retention period. Regulated utilities or pipelines often involve document retention periods of decades, sometimes over 50 years, often longer than the life of the plant.

Integrity-Checking Technologies

Passive integrity-checking technologies can be used to assess if a file has changed. These technologies include such mechanisms as hash values created by hash algorithms computed when a file is retrieved and if the file has changed. Unfortunately, passive integrity-checking technologies have no inherent mechanism to repair files and restore them to their original form; they can only alert you to the fact that a problem has occurred.

Active integrity-checking technologies can be used not only to assess if a file has changed but also (if appropriately configured) to restore a file to the original form as when it was stored. There are many proprietary examples of integrity-checking archive technologies. Because these technologies are generally well-understood and well documented, they are not discussed further here.

Long Term Physical *Information* Assets

When considering storage using physical mediums such as paper, it is important to ensure that the expected life of the storage medium exceeds the retention requirements. In the case of printed paper, the expected life of different types of paper, as well as different types of ink, can vary a great deal. It is also important to consider the storage conditions (such as humidity and temperature) required to ensure the ongoing integrity of the physical assets because this can affect the expected life of the physical storage medium.

APPENDIX D

The Quantitative/ROI Business Case

As discussed in the Commentary, a successful ***information governance*** approach requires both strategic commitment (adoption as an organizational priority) and tactical efforts. This Appendix discusses approaches to establishing an acceptable ROI for particular projects.

A typical ROI analysis weighs the benefits of a particular project against its cost, and calculates the length of time it will take to recoup the cost. The quantitative aspects of the business case are best determined by focusing on specific applications of ***information governance*** to identified problems or opportunities, or to discrete projects for implementation of the ***Information Governance*** program. [1]

The quantifiable benefits from pursuing ***information governance*** generally fall into four main categories: optimizing corporate value, risk reduction, hard cost avoidance, and soft cost avoidance.

Optimizing Corporate Value

Information governance can help make ***information*** assets available for new, valuable uses. It can also allow organizations to derive value from engaging in what might otherwise be cost-prohibitive endeavors, due to efficiencies and cost savings realized through ***information governance*** practices. In general, Gartner has identified the following as possible "adds" to corporate value from an ***Information Governance*** program:

. **Effectiveness**: Such as due to document-centric collaboration tools;

. **Cost/efficiency**: For example, from imaging/workflow solutions to replace traditional paper-oriented processes;

. **Customer service**: Such as from customer-relationship solutions that lead to better market penetration and customer satisfaction;

. **Competitive advantage**: As more modern tools and reliable ***information*** allows for speedier delivery of goods or services to customers; and

. **Revenue**: Such as a result of enhanced social media and web presences and solutions. [2]

> By way of example, a core benefit of an ***Information Governance*** program is to ensure that ***information*** used for different purposes across the enterprise -- e.g., for sales and marketing, but also for planning, billing, fulfillment, financial, customer feedback and other downstream purposes -- is reliable or trustworthy, accurate, and in formats usable across platforms or applications. Achieving these objectives requires that IT understand not only the business purposes and objectives but also whether data elements require special protections or treatments (e.g., for legal, RIM, privacy or security reasons). [3] Yet, oftentimes when a large organization initiates such a program, it finds that different business units or functions use different terminology for the same content concept. For example, an organization may refer to outside business partners as *vendors, suppliers, associates*, or *providers* and collect various ***information*** about such entities in systems that support particular functions within the organization. But if the terminology -- or application -- differs between and among business units, opportunities to cross-sell or otherwise leverage the ***information*** about the business partners may be missed. [4] Thus, an early goal for an ***Information Governance*** program may be to develop a common vocabulary and understanding of what ***information***-related assets exist; once that is done, the organization may realize that business advantages may be achieved -- at virtually no cost -- by cross-utilizing existing ***information*** or systems. [5]

Mergers and acquisitions, or technology upgrades, also present opportunities (and challenges) for improving data quality and corporate revenues by, for example, merging (and purging) customer lists to identify strong customers across multiple business lines. [6]

Risk Reduction

Risk reduction is also a significant benefit of ***information governance***. Business value may not be realized if an unanticipated risk creates an unexpected cost. For example, organizations may leverage ***information*** over the short-term (e.g., email for current communications), but once the ***information*** is no longer useful, the ESI is often stored away, rarely accessed, and often never re-assessed to determine whether the benefits of continued retention outweigh the risks. Thus, what was once a business asset may become a source of risk for certain organizational areas such as compliance or e-discovery, while providing little or no benefit for other organizational areas such as business units. Through proper ***information governance***, organizations can recognize these perils and elect to remediate the un- or under-utilized ***information*** assets, and optimize the business value of ***information*** while managing the associated risks.

Many types of adverse events can be avoided through effective ***information governance***. The value of risk reduction can be estimated by quantifying the potential losses that would result if an adverse event occurred and determining the reduced likelihood of such an occurrence due to effective ***information governance***. Some examples of risks posed by ***information*** assets follow:

a. Data Leakage: Many companies have valuable intellectual property that is more likely to be lost or leaked to the public and/or competitors if not properly managed through policies and procedures that emanate from a mature ***Information Governance*** program.

b. Privacy Breaches: A myriad of regulations applicable to particular sectors in the U.S. (e.g., HIPAA to health ***information***, GLBA to financial institutions, PERPA to federally funded educational institutions) require certain data to be protected and impose fines and other sanctions when the data is not properly protected or is improperly disclosed.

c. Security Lapses: Regulations such as the self-regulatory Payment Card Industry Data Security Standards require companies to protect credit card and other payment ***information***, or face fines.

d. Brand Impact: A breach of private customer ***information***, such as contact ***information*** or social security numbers, can adversely impact a company's brand and result in lost sales and/or consumer goodwill.

e. Litigation/Regulatory Risk: Access to the most relevant ***information*** at the inception of litigation or a regulatory inquiry may allow for an earlier and more accurate assessment of litigation risk, and thus, permit such events to be more effectively and economically managed.

Hard Cost Avoidance

Many benefits flowing from an ***information governance*** initiative are based on the premise that certain future costs can be delayed, reduced or avoided entirely because lesser volumes of data will be kept in a more efficient manner. These benefits can be quantified, and in an ***information governance*** initiative, often arise from the following areas:

a. Storage: Storage and maintenance costs can be radically reduced by the rationalizing data storage options, eliminating outdated ESI that no longer serves a legitimate business, legal or regulatory purpose, and moving valuable ***information*** that is occasionally and non-critically accessed to cheaper storage. A systematic approach to ***information governance*** may allow an organization to archive its less active and less critical data on less expensive tiers of storage, which in turn can eliminate unnecessary duplication of documents, associated backup overhead and better enable data disposition in line with organizational policy.

b. Outdated Backup Media: Eliminating the retention of large (and outdated) quantities of backup media, such as magnetic tapes, reduces the costs of backup media and related storage, labor and transfer expenses.

c. Personnel Costs: A successful ***Information Governance*** program will reduce the volume of ESI and make it easier to manage and to find ***information***. Accordingly, fewer personnel would be required to manage the reduced volume, allowing the organization to realign resources appropriately.

d. E-Discovery Costs: A reduced volume of electronic ***information*** can, in the event of litigation, reduce litigation costs *significantly*, because there will be less ***information*** to process and review. [7]

Soft Cost Avoidance

Other benefits resulting from improved ***information governance*** save time and effort that can be deployed for other activities. For example, having a more efficient method for storing and accessing email messages might save 30 minutes per day for each employee, netting a direct financial savings to the organization, or allowing employees to focus on more useful activities. Soft costs are often difficult to quantify, but the following are useful considerations:

a. Economies of Scale: Managing ***information*** on an *ad hoc* basis can result in requirements and risks being overlooked, benefits not being realized, and tremendous amounts of inefficiency due to the redundancy of effort this entails. Economies of scale can be realized by having an over-arching ***Information Governance*** program at an organizational level, which generates processes and procedures to govern how ESI is handled.

b. Organizational Inefficiencies: Organizations with excessive amounts of uncategorized ESI are often unable to locate needed ***information*** in a timely and efficient manner. An ***Information Governance*** program that creates an infrastructure for ***information*** assets promotes shorter client response times, allows the re-purposing of institutional knowledge, and enhances continuous improvement efforts.

Graphic

PHOTO 1 through 5, no caption, credit

The Sedona Conference Journal

End of Document

ARTICLE: INFORMATION GOVERNANCE: IT'S A DUTY AND IT'S SMART BUSINESS

Spring, 2013

Reporter
19 Rich. J.L. & Tech. 12

Length: 13948 words

Author: By Charles R. Ragan *

* Charles R. Ragan has practiced in high stakes commercial litigation for 30-plus years, and in the field of information management and electronic discovery for more than a decade. He was an original participant in Working Group 1 of The Sedona Conference, and has contributed to many of its publications, including: The Sedona Principles (2004 and 2007, and its Annotated Versions in 2004, 2005 and 2007), The Sedona Guidelines (2005), and The Case for Cooperation (2009). He has advised Fortune 500 companies, as well as emerging companies, on electronic discovery and records and information management issues. He is also an Adjunct Associate Professor at the University of Minnesota Law School, where he teaches a seminar on ***Information Governance***. He is licensed to practice law in California, Minnesota, and New York. The author thanks and acknowledges the editorial assistance of his colleague and friend, M. Kate Chaffee, in reviewing earlier drafts of this article, but he remains responsible for any error.

Highlight

Cite as: Charles R. Ragan, ***Information Governance****: It's a Duty and It's Smart Business*, *19 RICH. J.L. & TECH. 12 (2013), available at http://jolt.richmond.edu/v19i4/article12.pdf*.

Text

I. INTRODUCTION

P1 A scant generation ago (twenty-five years), the World Wide Web--"an internet-based hypermedia initiative for global information sharing" --was largely a laboratory phenomenon. [1] In 1994, the Clinton Administration urged world leaders to develop a global information superhighway, [2] and the Information Age raced upon us. Now, Facebook has more than one billion accounts and most of us are constantly deluged by volumes of electronic information through e-mail, texts, social media, the Internet, cable systems, and others.

P2 Information is among the most valuable assets for most organizations--public or private. For some, the value may lie in priceless intellectual property, such as patents or trade secrets. For others, it may be a customer database built up over decades of sales or the brainchild of a Harvard student aggregating faces. For still others, it may be complex workflows or systems for transmitting demand for power from individual customers onto a regional grid for the distribution of electricity. Last but not least, and increasingly so, it may be a set of algorithms for assessing vast volumes of data and discerning what trades are most likely to succeed, or what products may appeal to a customer with discretionary income.

---

[1] *Tim Berners-Lee*, W3C, *http://www.w3.org/People/Berners-Lee/* (last visited Feb. 23, 2013) (dating the invention of the World Wide to 1989).

[2] *See* Jube Shiver Jr., *Gore to Call for Global Information Age*, L.A. TIMES (Mar. 17, 1994), *http://articles.latimes.com/1994-03-17/business/fi-35298_1_economic-development*.

P3 For most of the Information Age, it has been relatively risk-free to allow these volumes of information to accumulate--even after their normal useful life - because storage devices have been cheap. In fact, the cost of unit storage declined approximately ninety-nine percent from 2000 to 2010. [3] So far, as the saying goes, this is "all good." But recently, three important caveats have injected themselves into that bromide. First, the total worldwide costs to store and manage the ever increasing volumes of information being generated and retained in organizations are *increasing*. [4] The increase in volumes is truly staggering. It was estimated in 2011 that ninety percent of the data in the world had been created in the prior two years and for most organizations, information volume doubles every eighteen to twenty-four months. [5]

P4 Second, absent investment in costly search technologies capable of federated searches across platforms and storage containers, these volumes of information may jeopardize the organization's ability to retrieve valuable information efficiently such that strategic opportunities are lost. Third, if information is retained past its useful life (*i.e.*, after its business function is fulfilled and while there is no other legal obligation to keep it), that information could be subject to future requests in litigation or governmental investigation. [6] As a recent article notes, while the basic cost to manage a terabyte of information may be about $ 5,000, if that terabyte is retained unnecessarily and becomes the subject of discovery (and collection, processing, analysis, and review), that unneeded data may cost the organization an extra $ 15,000. [7] For an organization that has petabytes of information (roughly 1,000 times a terabyte), or in the case of our largest organizations, scores of petabytes, the "electronic discovery tax" poses a horrific and unnecessary risk. [8]

P5 For some in senior management (*i.e.*, those in the Boomer generation), the problem of unnecessary data causing substantial costs in litigation will sound familiar. In fact, as a result of expensive paper discovery experiences in the 1970s and 1980s, many organizations developed policies falling under the euphemistic label of "document retention" or "record retention" policies. [9] Under these policies, an organization established how long they *had* to keep certain information due to laws or regulations, how long they *wanted* to keep information due to business value or need, and destroyed what they did not have or want to keep. [10] The Supreme Court famously

---

[3] Barclay T. Blair, *Today's PowerPoint Slide: The Origin of* ***Information Governance*** *By the Numbers*, BARCLAY T. BLAIR (Oct. 28, 2010), *http://barclaytblair.com/2010/10/28/origins-of-**information-governance**-powerpoint/* (referring to data from the IDC*Quarterly Storage Software Tracker, Worldwide Quarterly Disk Storage Tracker* and *Costs of Hard Drives 1956-2010*).

[4] *See id.* While the worldwide expenditures on storage hardware remained the same, expenditures on storage software more than doubled between 2000 and 2010.

[5] DEIDRE PAKNAD & RANI HUBLOU, CGOC, INFORMATION LIFECYCLE GOVERNANCE LEADER REFERENCE GUIDE 5 (2012), *available at https://www.cgoc.com/files/CGOC_ILG_LeaderReferenceGuide.pdf*.

[6] *See* Thomas M. Jones et al., *Going Global: Mapping an International Records Retention Strategy*, ZASIO ENTERPRISES 2, *http://www.zasio.com/pdfs/consulting_goingglobal.pdf* (last visited Feb. 24, 2013).

[7] Jake Frazier & Anthony Diana, *'Hoarders': The Corporate Data Edition*, LAW TECH. NEWS (Dec. 19, 2012), *http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202581938140&Hoarders_The_Corporate_Data_Edition&slreturn=20130109125622*. Actually, the number cited in the article is probably low, as the author's calculation appears to assume equal volumes are collected, processed, and reviewed; when in fact far more data is collected and processed than is reviewed.

[8] For an organization with 40 petabytes of data under management, the potential "tax" would be $ 600 million! (40 *times* 1,000 *times* $ 15,000 = $ 600,000,000).

[9] *Cf.* STEVE PALOMINO & ART VANCIL, AICPA, A PRACTICE AID FOR RECORDS RETENTION (2012), *available at http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/BusinessIntelligence/DownloadableDocuments/Records_Retention_Mktg.pdf* (discussing the importance of record retention policies and suggesting practice tips for implementing such policies).

[10] *See id.* at 5.

ruled in *Arthur Andersen*, a case that grew out of the Enron scandal, that such policies are perfectly lawful. [11] In fact, the Court in that case recognized that such policies are "created in part to keep certain information from getting into the hands of others, including the Government," and stated that a manager may instruct his employees to comply with a valid document retention policy under normal circumstances. [12] In the day of paper records, relatively small staffs with administrative assistance in local offices could administer such policies.

P6 By the late 1980s and early 1990s, however, competitive pressures of globalization forced many organizations in the United States to go lean; consequently, many records functions were cut as expendable. [13] More problematic, however, were the advent of the Information Age and the proliferation of "road warriors" who wanted all of their potentially relevant files stored on their laptops. Few organizations took immediate steps to update their retention policies to account for the influx of electronic records. Further, in those organizations that sought to maintain "retention" policies for all information regardless of the media, those developments turned most employees into *de facto* records managers without any additional compensation or training in the discipline. [14] Some workers tried to remain faithful to the policies, but as the volumes exploded in recent years, knowledge workers were spending more than a quarter of their time managing e-mail. [15] In a competitive global economy, this is a not a model of efficiency. As Jason Baron, the 2011 recipient of the prestigious Emmett Leahy award, persuasively urged, "[W]e need to declare an official end to the end-user being expected to act as *de facto* records manager." [16]

P7 The glut of information arriving randomly also interferes with productivity. One study showed that, on average, knowledge workers are interrupted every three minutes and it takes a half hour to return to the pre-interruption level of concentration. [17] This is no small problem. Indeed, the problem has led senior researchers at some of the world's leading technology companies to form (and incorporate) the Information Overload Research Group. [18]

---

[11] *Arthur Andersen LLP v. United States, 544 U.S. 696, 704 (2005).*

[12] *Id.* Once litigation or government inquiry is reasonably anticipated, however, one ventures into the realm of circumstances that are not "normal." *See, e.g.*, *Hynix Semiconductor, Inc. v. Rambus, Inc., 645 F.3d 1336, 1344 (Fed. Cir. 2011); Micron Tech., Inc. v. Rambus, Inc., 645 F.3d 1311, 1319 (Fed. Cir. 2011).*

[13] *Cf.* Jones et al., *supra* note 6 ("An organization's goal should be to retain *only* those records needed to conduct business, to comply with the law . . . and to reasonably preserve archival documentation") (emphasis added).

[14] *See* R. Thomas Howell & Rae N. Cogar, *Records Retention -- An Essential Part of Corporate Compliance*, *in* RECORD RETENTION AND DESTRUCTION CURRENT BEST PRACTICES 1, 4 (Am. Bar Ass'n ed., 2003), *available at* *http://www.americanbar.org/content/dam/aba/migrated/buslaw/newsletter/0021/materials/recordretention.authcheckdam.pdf* (noting a widely applied rule that the creator of electronic documents has the responsibility for retaining the document).

[15] Published estimates range from 28% to 50%. *Compare* Laura Vanderkam, *Stop Checking Your Email, Now.*, CNN MONEY (Oct. 8, 2012, 11:14 AM), *http://management.fortune.cnn.com/2012/10/08/stop-checking-your-email-now/*, *with* Courtney Rubin, *Study: Employees Are Unproductive Half the Day*, INC. (Mar. 2, 2011), *http://www.inc.com/news/articles/201103/workers-spend-half-day-being-unproductive.html* (finding that employees at small and medium-sized businesses spend half their day working un unproductive tasks such as filtering information and correspondence).

[16] *See* Jason R. Baron, Acceptance of the 2011 Emmett Leahy Award 7 (Sept. 15, 2011), *available at* *http://www.emmettleahyaward.org/uploads/Proceedings_2011.pdf*.

[17] *See* L. Gordon Crovitz, *The Information Age: Unloading Information Overload*, WALL ST. J., July 7, 2008, at A11.

[18] *See id.*; *About IORG*, INFO. OVERLOAD RES. GROUP, *http://iorgforum.org/about-iorg/* (last visited Feb. 20, 2013).

P8 Another exacerbating factor in the modern organization is that some users who are newer to the workplace have not received training about the risks of quickly (and informally) generating information that might prove problematic for the organization in litigation. [19]

P9 Finally, the challenge of dealing with information in the modern organization is a dynamic, not stationary, target because the technologies that generate and deliver information are constantly changing. Witness, for example, the quick sprint from paper documents and phone-message slips, to e-mail and voicemail, through universal messaging, or instant messaging and chat, and to Facebook, LinkedIn, and Twitter. [20]

P10 Something new--and at least a *little* different--is needed if we are to avoid what Baron and others have called "the coming 'digital Dark Ages'" in which we cannot see clear paths forward due to the glut of information before us. [21] Thus far, those who labor principally in the fields of law and records management have started to discuss these issues, but have found difficulty gaining traction or budget, usually for want of either a champion or a clear business case with an indisputable return on investment. As discussed below, senior management in all organizations and corporate boards of directors need to recognize that assessing and overseeing management of the risks posed by information overload *is* a necessary part of their existing duties.

II. THE FOUNDATIONS OF THE DUTIES

P11 The board of directors of a corporation is generally responsible for overseeing the business of and helping to set strategy for the corporation so as to minimize unnecessary risks. Senior management is generally responsible for managing the company and executing in accordance with the organization's strategic direction. Board members have fiduciary duties to the owners of the corporation (its shareholders), which include the duty of care, the duty to remain informed, and the duty of loyalty, as typically circumscribed by the so-called "business judgment rule." [22]

P12 Several courts have elaborated on these duties in factual circumstances not stemming from an organization's management of information-related issues, but in terms that are directly relevant to the current state of ***information governance*** in many organizations. [23] The principles thus enunciated raise the specter of potential liability if officers and directors utterly fail to ensure the adequacy of information systems. For example, in *Caremark International Inc. Derivative Litigation*, plaintiffs claimed that "directors allowed a situation to develop and continue which exposed the corporation to enormous legal liability and that in doing so they violated a duty to be active monitors of corporate performance." [24] The Delaware Chancery Court, noting that the theory advanced was "possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment," nonetheless agreed that director liability for breach of the duty of care could arise either from a board decision that resulted in loss or "from an *unconsidered failure of the board to act* in circumstances in which due attention would, arguably, have prevented the loss." [25] In discussing the "business judgment rule" limitations on these principles,

---

[19] *Cf.* Teresa Schoch, *Turning the Ship Around with Four-Generation Crew*, INFO. MGMT. MAG., July-Aug. 2012, at 28 (noting the importance for younger generations to realize "how critical the implementation of record capture procedures is to the organization's long-term well-being").

[20] Even Pope Benedit XVI was on Twitter--in eight languages. *See* Gaia Pianigiani & Rachel Donadio, *Twitter Has a New User: The Pope*, N.Y. TIMES (Dec. 3, 2012), http://www.nytimes.com/2012/12/04/world/europe/follow-the-pope-on-twitter-he-follows-no-one.html?_r=0. Pope Francis has also joined Twitter.*See Pope Francis*, TWITTER, twitter.com/Pontifex (last visited May 13, 2013).

[21] Jason R. Baron, *supra* note 16, at 8.

[22] *In re Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 967-68 (Del. Ch. 1996).* Under the business judgment rule, directors are generally insulated if they have considered an issue in good faith or through a rational and informed process.

[23] *See generally id.*; *in re* *Abbott Labs. Derivative S'holder Litig., 325 F.3d 795 (7th Cir. 2003).*

[24] *See* *698 A.2d at 967.*

[25] *Id.*

Chancellor Allen concluded, in line with Judge Learned Hand's analysis, "the core element of any corporate law duty of care inquiry [is] *whether there was good faith effort to be informed and exercise judgment*." [26] With respect to potential liability for failure to monitor, Chancellor Allen stated:

> [A] director's obligation includes a duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists, and that failure to do so under some circumstances may, in theory at least, render a director liable for losses caused by non-compliance with applicable legal standards. [27]

P13 In the years since *Caremark* was decided, much has happened in the world of corporate governance. The case has been cited more than 3,000 times; [28] many courts have embraced the decision, a few have commented negatively or distinguished the case, and some have found on the facts before them the "unconsidered failure of the board to act" required for liability. [29]

P14 Perhaps even more important, Americans have already witnessed two separate periods of corporate malfeasance in this century. The first of these periods included such fiascos as Enron and WorldCom [30] while the second stemmed from the overvaluation and trading of subprime mortgages, which led to the demise of several major financial institutions and the global financial crisis of 2008. [31] Both led to outcries for heightened scrutiny on corporate America and each led to new legislation imposing new requirements on corporations. The first led to the passage of the Sarbanes-Oxley legislation [32] and the second led to the passage of the Dodd-Frank legislation. [33]

P15 Posed squarely, the issue is whether the risks attending information systems in the modern enterprise are such that directors and senior management may safely ignore them and fail to take steps to enhance ***information***

---

[26] *Id. at 968* (citing *Barnes v. Andrews, 298 F. 614, 618 (S.D.N.Y. 1924))* (emphasis added). In *Barnes*, Judge Learned Hand noted that directors are not specialists; rather, they are "the general advisors of the business, and if they faithfully give such ability as they have to their charge, it would not be lawful to hold them liable." *Barnes, 298 F. at 618.*

[27] *698 A.2d at 970.* The *Caremark* court concluded that the board had followed procedures to inform themselves regarding contracts with health care providers, so as to be protected by the business judgment rule, and approved the settlement in issue.

[28] As of April 23, 2013, Westlaw's Keycite shows 3,234 citations to the case, including 260 cases.

[29] *E.g., In re Abbott Lab. Derivative S'holder Litig., 325 F.3d 795, 808-809 (7th Cir. 2003)* (finding that six years of noncompliance established lack of good faith).

[30] *See* MARK JICKING & BOB LYKE, CONG. RES. SERV., RS21253, WORLDCOM: THE ACCOUNTING SCANDAL 1-2 (2002), *available at http://www.iwar.org.uk/news-archive/crs/13384.pdf*.

[31] *See generally*, KATALINA M. BIANCO, CCH, THE SUBPRIME LENDING CRISIS: CAUSES AND EFFECTS OF THE MORTGAGE MELTDOWN (2008), *available at http://www.business.cch.com/bankingfinance/focus/news/Subprime_WP_rev.pdf*.

[32] *See generally* Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, ***116 Stat. 745 (2002).***

[33] *See generally* Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, ***124 Stat. 1376 (2010).*** The act applies not just to financial institutions, but to all organizations doing business in the financial, capital, and credit markets, including energy companies, electric and natural gas utilities, chemical companies, mining and mineral companies, airlines, agribusinesses, and consumer products companies. *See* Fred Pulzello & Sonali Bhavsar, *Dodd-Frank Act Puts Focus on* ***Information Governance***, INFO. MGMT. MAG, Nov.-Dec. 2011, at 42, *available at http://content.arma.org/IMM/Libraries/Nov-Dec_2011_PDFs/IMM_1111_business_matters_dodd_frank_act_puts_focus_on_info_gov.sflb.ashx*. As recently as December 2012, the Government Accountability Office estimated that rulemaking under the Dodd-Frank legislation was only half complete.*See Fragmented U.S. Regulatory System Stalls Dodd-Frank Rules-GAO*, REUTERS (Jan. 23, 2013), *http://www.reuters.com/article/2013/01/23/financial-regulation-gao-idUSLIN0ASHV320130123*.

governance processes. [34] The short answer, I submit, is a resounding "no." As one commentator observed, "[t]here is no doctrinal reason Caremark claims should not lie in cases in which the corporation suffered losses, not due to a failure to comply with applicable laws, but rather due to lax risk management." [35] The three following sections, respectively, (a) describe those risks, [36] which include some conflicting obligations, (b) suggest a logical approach for addressing the risks, and (c) identify the opportunities with existing mechanisms for addressing them.

III. RISKS ASSOCIATED WITH INFORMATION IN THE MODERN ENTERPRISE

A. The Risks Are Many and Diverse

P16 The risks associated with information in the modern enterprise are numerous, varied, and conflicting. At the outset, one should also note that almost all information is now created electronically [37] and because electronic information has significant differences from paper documents, former processes and paradigms are no longer 1:1 analogs. [38] Briefly stated, the risks associated with information in the modern enterprise include [39] :

. Proprietary information. Information that has competitive value must be protected against disclosure or misuse. In most organizations, there will be several levels of confidentiality or protection requiring different treatments (*e.g.*, company-private, confidential, highly confidential, etc.). [40]

. Contractually protected information. When considering new business arrangements or technologies, organizations often receive information under the terms of non-disclosure agreements. Such contractual obligations with third parties also require protection of such information from misuse or theft. [41]

. Challenges to sound record keeping practices. Information that has business value to an organization should be maintained in such a manner as to ensure its accuracy, integrity, and availability for later use, but also

---

[34] The problem is not limited to business organizations. Indeed, in a 2011 memorandum on managing government records, President Obama warned that "if records management policies and practices are not updated for a digital age, the surge in information could overwhelm agency systems, leading to higher costs and lost records." Memorandum from President Barack Obama on Managing Gov't Records for Heads of Exec. Dep'ts and Agencies (Nov. 28, 2011), *available at* http://www.whitehouse.gov/the-press-office/2011/11/28/presidential-memorandum-managing-government-records. The government initiative is certainly needed and welcome, but there should be no mistake that the problem is not limited to a records management issue.

[35] Stephen M. Bainbridge, Caremark *and Enterprise Risk Management*, 34 J. CORP. L. 967, 968 (2009).

[36] Bainbridge further observes, "risk management does not differ in kind from legal compliance or accounting controls." Id. at 981.

[37] Recent estimates suggest that more than ninety-nine percent of all information is now generated electronically. *See* ROBERT M. VERCRUYSSE & GREGORY V. MURRAY, VERCRUYSSE MURRAY & CALZONE, P.C., ELECTRONICALLY STORED INFORMATION AND THE NEW FEDERAL RULES OF CIVIL PROCEDURE REGARDING DISCOVERY 1 (2007), *available at* http://www.vmclaw.com/articles/3_Electronic_discovery.pdf.

[38] *See generally Introduction* to THE SEDONA CONFERENCE(R), THE SEDONA PRINCIPLES: BEST PRACTICES RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION (2nd ed. 2007), https://thesedonaconference.org/download-pub/81 [hereinafter "The Sedona Principles"] (providing a brief but informative survey of differences between paper and electronic information).

[39] This is an illustrative--not an exhaustive--list.

[40] *See Excerpt from Dupont Records Management Guide*, *in* RECORDS RETENTION AND DESTRUCTION CURRENT BEST PRACTICES 22, 28 (Am. Bar Ass'n ed., 2003), available at http://www.americanbar.org/content/dam/aba/migrated/buslaw/newsletter/0021/materials/recordretention.authcheckdam.pdf.

[41] *See* JERE M. WEBB, A PRACTITIONER'S GUIDE TO CONFIDENTIALITY AGREEMENTS 1 (1985), *available at* http://www.stoel.com/files/confidentialityagreementguide.pdf.

protected against alteration. Keeping excessive volumes of information, which might not adequately distinguish drafts from finals, undermines these objectives. [42]

. E-Discovery. Information that may be responsive to requests in U.S. litigation or investigation must be identified quickly and preserved once a claim (or inquiry) is reasonably anticipated. [43]

. Challenges in developing and implementing retention policy schedules. Separate from any litigation or investigation obligation to retain information, an organization is required to retain different categories of information for various periods, depending on the jurisdictions where the organization does business and the nature of those businesses. Determining the retention schedule for a given organization through traditional methods of legal research is a labor-intensive and expensive effort. [44] In the case of a global enterprise, for example one doing business in 130 countries, the expense could easily exceed one million dollars and the retention requirements found for different jurisdictions often conflict, even for a single category of information. Finally, traditional means for categorizing information into record series that can be manually segregated, stored, retrieved, and eventually destroyed do not translate well or efficiently into the world of electronic storage, retrieval, and disposition.

. Data protection and privacy. Numerous jurisdictions outside the United States have adopted comprehensive regulations for data protection and privacy regarding "personally identifiable information," which is broadly defined to include even information in an e-mail header. [45] The best known of these regimes is in the European Union and its constituent nation states. [46] Legislation or initiatives have also been launched in Asia (Singapore, South Korea, Taiwan, Malaysia, India, Vietnam, New Zealand, Hong Kong, and China) and Latin America (Brazil, Mexico, Peru, Colombia, Uruguay, and Costa Rico). [47] Typically, such information should be retained only as long as necessary to fulfill its purpose, but enforcement of privacy regulations varies widely from one jurisdiction to another (and even within the European Union). [48] In the United States, there is a patch quilt of federal and state, non-uniform legislation (and some state constitutions) protection of privacy interests

---

[42] *See generally The Generally Accepted Recordkeeping Principles*, ARMA (Feb. 17, 2013), http://www.arma.org/garp/index.cfm. These Principles were previously marketed under the term GARP; ARMA recently has shied away from referring to them as "GARP" because of trade name issues raised by the Global Association of Risk Professionals.

[43] *See* The Sedona Conference(r), *The Sedona Conference Commentary on Legal Holds: The Trigger & The Process*, 11 SEDONA CONF. J. 265, 267 (2010).

[44] In the author's experience, a client could easily spend $ 10,000 per state jurisdiction in legal fees for this research. *See also* Charles Ragan, *How to Avoid the Information Management Dark Ages*, LAWTECH. NEWS 1, 2 (Dec. 16, 2011), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202535755654&How_to_Avoid_the_Information_Management_Dark_Ages.

[45] Gail Lasprogata, et al., *Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada*, 2004 STAN. TECH L. REV 4, P 14 (2004) available at http://stlr.stanford.edu/STLR/Articles/04_STLR_4. *See generally* ERIKA MCCALLISTER ET AL., GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION § 2-2 (2010).

[46] Lasprogata, *supra* note 45, at P 113.

[47] *See generally* Matthew Glynn, *Australia: Data Privacy Compliance in Asia Pacific*, MONDAQ (Nov. 17, 2012), http://www.mondaq.com/australia/x/206518/data+protection/DATA+PRIVACY+COMPLIANCE+IN+ASIA+PACIFIC; Aldo M. Leiva,*Data Protection Law in Spain and Latin America: Survey of Legal Approaches*, 41 INT'LL. NEWS 4 (2012), http://www.americanbar.org/publications/international_law_news/2012/fall/data_protection_law_spain_latin_america_survey_legal_approaches.html.

[48] *See generally European Data Privacy Obligations Impact On U.S. Businesses*, NICOLAI LAW GROUP, P.C. (Aug. 1, 2001), www.niclawgrp.com/Resource-Materials/Montlily-Memo/European-Data-Privacy-Obligations-Impact-On-U-s-Businesses.shtml.

in specific areas. [49] In addition, most states have adopted legislation specifying what steps an organization must take in the event that its information systems with consumer information are breached. [50] In short, most organizations face a web of potentially conflicting and constantly changing privacy obligations that must be comprehended and respected.

. Conflict between data protection regulation and traditional U.S. expectations of "liberal" pretrial discovery. The privacy or data protection rules and regulations of many jurisdictions do not permit "processing" or "transfer" of personal information without the consent of the data subject. (A proposed data protection reform in the European Union would ensure that explicit consent be given before a company could process a data subject's personal data. [51]) These regulations often conflict with the expectations of judges in the United States that all information relevant to the claims and defenses in an action (if not the subject matter of the litigation) will be freely exchanged during discovery. [52]

. Enhanced risk of security breaches, and attendant release of personal information, including health and financial information. [53]

. Ever-changing landscape of technologies that enhances business communications and confounds management of electronically stored information. Modern technologies--including social media and smart devices (*i.e.*, tablets and smartphones)--allow for the immediate transfer of data and images to unlimited numbers of people who are virtually in any place on the planet with just a few clicks or swipes of the finger. These developments pose obvious risks to sensitive organizational information, including trade secrets and other intellectual property. [54]

. Trend to allow workers to BYOD. In order to attract the best and brightest young talent, many organizations are succumbing to pressures to allow employees to Bring Your Own Devices to work. [55] The introduction of these devices into the workplace presents a host of issues for an organization's central technology function. [56]

---

[49] *See, e.g.*, The Children's Online Privacy Protection Act of 1998, *15 U.S.C. §§ 6501-6506* (2006); Electronic Communication Privacy Act of 1986, *18 U.S.C. §§ 2510-2511* (2006); The Health Insurance Portability and Accountability Act of 1996, *42 U.S.C. § 1320a-7c*; Health Information Technology for Economic and Clinical Health Act, *42 U.S.C. §§ 17931*, *17937* (2006 & Supp. III 2010).

[50] *See* GINA STEVENS, DATA SECURITY BREACH NOTIFICATION LAWS, Summary (2012), *available at https://www.fas.org/sgp/crs/misc/R42475.pdf*.

[51] *See* EUROPEAN COMM'N, HOW DOES THE DATA PROTECTION REFORM STRENGTHEN CITIZENS' RIGHTS? 1 (2012), *available at http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf*.

[52] *See* AMERICAN BAR ASSOCIATION SECTION OF INTERNATIONAL LAW, REPORT TO THE HOUSE OF DELEGATES 103, 1-2 (2012), *available at http://www.abanow.org/2012/01/2012mml03/*.

[53] *See infra* Part IV.B.3.

[54] *See* PRICEWATERHOUSECOOPERS LLP, SECURITY FOR SOCIAL NETWORKING 1 (2008), available at *http://www.pwc.com/en_US/us/it-risk-security/assets/social-networking-final.pdf*.

[55] *See generally* Brittany Bolster, *BYOD: Bring Your Own Device to Work*, AMERICA'S REMOTE HELP DESK BLOG (Dec. 5, 2012), *http://www.remotehelpdesk.com/uncategorized/byod-bring-your-own-device-to-work/*.

[56] *See, e.g.*, Emily Maltby, *Many Gadgets, Many Risks*, WALL ST. J. (Nov. 11, 2012), *available at http://professional.wsj.com/article/SB10001424052970204840504578087311857039762.html?mg=reno64-wsj* (noting that smaller companies may be earlier adopters of BYOD policies in part because that helps them lower IT costs).*See generally* Brent Gatewood, *The Nuts and Bolts of Making BYOD Work*, INFO. MGMT. MAG. (Nov./Dec. 2012), *available at http://content.arma.org/IMM/Libraries/Nov-Dec_2012_PDFs/IMM_1112_Making_BYOD_Work.sflb.ashx*; Nancy D. Barnes & Frederick Barnes,*Smartphone Technologies Shine Spotlight on* ***Information Governance***, INFO. MGMT. MAG. (May/June

In the past, for example, the organization could concentrate on a few technology platforms running a particular operating system that relied on a dedicated backend server environment. The proliferation of smart devices, however, introduces the need for some conversancy with Apple and Android operating systems and the development of new security protocols to account for them. In addition, to the extent information on such devices may be called for in litigation or investigation, the organization (or its vendors) will have to become familiar with an array of ESI harvesting techniques because collection techniques typically vary from device to device and from operating system to operating system. [57]

. Movement to cloud alternatives. Some organizations, in order to take advantage of economies of scale and resulting economic savings, have considered moving their data "into the cloud" where it may be commingled with data of other organizations and is not under the immediate possession or control of the organization (which may impair the ability to respond to requests in litigation or evaluate claims of internal malfeasance). [58] The economics of cloud operations can be incredibly attractive (if not compelling) for some organizations and/or functions, but there are also a variety of risks--including mid- to long-term costs--that should be analyzed and evaluated. [59]

. Legacy or "debris" data that has no "owner" or continuing value. As noted above, if the organization does not dispose of data and information after its useful life (and when it is not subject to a duty to preserve for litigation or investigation), but instead allows it to linger, the organization will be spending money to store and manage information with no business value [60] *and* that information may be subject to costly future discovery requests. Because "storage has traditionally been cheap" [61] --at least in relative terms--this legacy or "debris" data is a significant risk and problem for many organizations.

. "Big Data." Lastly, and taking the opposite side from the last point, several large organizations are grappling with the issue of so-called Big Data, *i.e.*, whether or not to keep lots of data and subject it to sophisticated algorithms and searching techniques that can produce significant business opportunities and sales. [62]

2012), *available at* http://content.arma.org/IMM/Libraries/May-June_2012/IMM_0512_Tech_Trends_Smartphone_Technologies.sflb.ashx.

[57] *See* Greg Buckles, *A Quick Forensics Lesson: The Smart Phone Is Much More than Just a Hard Drive*, LEGAL IT PROF'LS (July 17, 2012), http://www.legalitprofessionals.com/index.php/col/guest-columns/4471-a-quick-forensics-lesson-the-smart-phone-is-much-more-than-just-a-hard-drive.

[58] Rackspace Support, *Moving Your Infrastructure to the Cloud: How to Maximize Benefits and Avoid Pitfalls*, RACKSPACE, http://www.rackspace.com/knowledge_center/whitepaper/moving-your-infrastructure-to-the-cloud-how-to-maximize-benefits-and-avoid-pitfalls (last updated Sept. 12, 2012).

[59] For example, is the cloud provider capable of (a) preserving and providing data to the owner quickly enough for the owner to respond to discovery requests, or (b) disposing of data in accordance with the owner's retention policy.

[60] The costs of managing information include the cost of labor and equipment to backup data pursuant to disaster recovery and business continuity protocols. Those organizations that do not know what information they have in their legacy systems are paying to backup valueless information.

[61] Mary E. Shacklett, *'Big Data' Calls for an IT Culture Change*, INTERNET EVOLUTION (Mar. 11, 2010), http://www.internetevolution.com/author.asp?section_id=562&doc_id=188999.

[62] Analysis of big data may result in enormous potential savings. For example, the *Economist Outlook for 2012* refers to a McKinsey Global Institute study indicating that analysis of health care data could yield $ 300 billion worth of savings in the United States alone. Ludwig Siegele, *Big Welcome to the Yotta World*, ECONOMIST (NOV. 17, 2011), http://www.economist.com/node/21537922. Big data also has a wide variety of uses.*See, e.g.*, Joseph Walker, *Meet the New Boss: Big Data*, WALL ST. J. (Sept. 20, 2012, 11:16 AM), http://online.wsj.com/article/SB10000872396390443890304578006252019616768.html (hiring employees); Catherine Dunn,*IBM's New Privacy Chief Eyes Big Data, Analytics*, LAW (Oct. 17, 2012), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1350226328616&rss=rss_ltn_news (tailoring customer offers and services); Evgeny Morozov,*The Tyranny of Algorithms*, WALL ST. J. (Sept. 20, 2012, 12:15 AM), http://online.wsj.com/article/SB10000872396390443686004577633491013088640.html (picking the next pop-music star).

P17 From this recitation it should be apparent that while these issues may be present for most organizations, the strategies one organization may choose to follow, and the acceptance or mitigation of particular information-related risks, will differ from the next, depending on each organization's business objectives, specific legal obligations, and its tolerance for risk. For example, a company like Google or Facebook may have an interest in maximum retention of personal demographic information so as to match the ads it displays in sidebars to a particular user, while a manufacturer of heavy equipment might not wish to capture and retain user information for every visit to a webpage advertising forklifts. Senior management and corporate boards have a responsibility to ensure that the organization considers these diverse information-related issues and the optional approaches surrounding them so that the organization addresses them in line with its overall goals and strategies, rather than in an ad hoc manner driven by a single (or even a spare few) disciplinary biases.

B. Organizations Often Assert that They Handle All Information Appropriately

P18 In response to heightened scrutiny of corporate behavior, many organizations have "gone on offense" to assure shareholders that their interests are being managed well. [63] Thus, many organizations have adopted "codes of conduct" that recognize that a global company must comply with the laws of many countries and that each employee is responsible for knowing and complying with the letter and spirit of applicable laws or regulations. [64] Many organizations also speak in their public materials about the duty to protect confidential information and to take precautions before sharing it with anyone, [65] the need to protect company assets to guard its competitive advantage in the marketplace, the importance of "us[ing] electronic communications wisely," and the expectation that each employee is responsible for maintaining accurate records and complying with company policies and procedures for recordkeeping. [66] Some even recognize that employees have a "right to engage in social, professional and political dialogue outside the workplace" through, for example, social media. [67]

P19 These broad statements [68] set a high bar of expectations. The next obvious questions are whether there are mechanisms in place to facilitate compliance by individual employees or associates, and whether the board has attempted to assure itself that they are adequate.

C. Surveys Strongly Indicate That the Reality Is Far from the Promise

P20 Surveys of knowledgeable persons suggest that reality falls far below the publicly stated promise. For example, a recent survey found that lack of proper management of information was "impacting business productivity and creating costs and liabilities." [69] As Baron and others have observed, employees are spending too much time

---

[63] *See, e.g.*, James E. Rohr, *Message from the Chairman*, PNC (Mar. 7, 2012), *available at* http://phx.corporate-ir.net/phoenix.zhtml?c=107246&p=irol-chairman2012 (follow "Annual Letter to Shareholders" hyperlink) ("At PNC we manage our business with the goal of creating opportunities for increased shareholder value over the long term.").

[64] *See, e.g.*, *Code of Conduct*, JPMORGAN CHASE & Co. (Mar. 15, 2012), *available at* http://www.jpmorganchase.com/corporate/About-JPMC/document/2012CodeofConduct_05_15_12_ada.pdf [hereinafter JPMorgan Chase Code] (discussing compliance with the law in section 1.3);*Intel Code of Conduct*, INTEL (Jan. 2013), *available at* http://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/policy-code-conduct-corporate-information.pdf (requiring employees to conduct business with honesty and integrity and to follow the letter and spirit of the law).

[65] *E.g.*, JPMorgan Chase Code, *supra* note 64, at 5.

[66] *Id.* at 22-23.

[67] *Id.* at 31, 34 (outlining employees' responsibilities).

[68] In the author's experience, such statements are typical of large organizations and can readily be found in corporate governance materials on the Internet.

[69] *The Information Explosion: How Organizations Are Dealing with It*, COUNCIL FOR INFO. AUTO-CLASSIFICATION 3 (Oct. 2011), http://www.infoautoclassification.org/survey.php.

searching and managing information and recreating desired information that is not readily retrievable. [70] In fact, one recent survey reported that seventy-four percent of respondents reported that valuable information was being lost, and seventy-three percent said that their organizations missed business opportunities because they could not access information efficiently. [71] Virtually all organizations responding to the survey acknowledged rapid volume growth of electronic information: eighty-one percent said document management environments were challenging to manage, seventy-eight percent admitted increased IT infrastructure costs, and eighty-eight percent said they had large stores of legacy data. [72]

P21 Significantly, an increasing and sizeable percentage of senior corporate personnel recognize that their valuable information is *not* secure. For example, in a 2010 study, thirty-seven percent said they were not confident that their electronic records had not been modified, deleted, or inappropriately accessed. [73] Just two years later, forty-eight percent of directors and fifty-five percent of general counsel (of more than 13,000 surveyed) cited data security as an issue of concern, making it the most referenced concern. [74] Another study estimated the median annualized cost of cyber crime per company at $ 5.9 million. [75] But these direct costs related to a data breach (Sony reportedly spent more than $ 170 million to address multiple breaches in 2011 [76]) pale in comparison to the total injury, including that to the company's reputation. [77]

P22 Some of the cybersecurity risk can be attributed to criminal activity (*e.g.*, identity theft), but some apparently is the result of international espionage or politically motivated retaliation. [78] Further, in 2013, several major news organizations acknowledged that their systems had been hacked and their journalists' e-mail passwords

---

[70] *Id.*

[71] *Id.* at 5.

[72] *Id.* at 4-7. Legacy data is the term used to describe information past its useful life, or with no clearly identifiable owner.

[73] *E-Discovery and ERM: How Is Records Management Performing in the New Spotlight?*, AIIM MARKET INTELLIGENCE, 4 (2010), http://www.aiim.org/Research-and-Publications/Research/Industry-Watcli/ERM-and-eDiscovery-2010.

[74] CORPORATE BOARD MEMBER, LEGAL RISKS ON THE RADAR 2 (2012), *available at* http://www.fticonsulting.com/global2/media/collateral/united-states/legal-risks-on-the-radar.pdf.

[75] *Second Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies*, PONEMON INSTITUTE 1 (2011), http://www.hpenterprisesecurity.com/collateral/report/2011_Cost_of_Cyber_Crime_Study_August.pdf.

[76] *See* Mathew J. Schwartz, *Sony Data Break Cleanup To Cost $ 171 Million*, INFORMATIONWEEK (May 23, 2011), http://www.informationweek.com/security/attacks/sony-data-breach-cleanup-to-cost-171-mil/229625379.

[77] *See* Juro Osawa, *As Sony Counts Hacking Costs, Analysts See Billion-Dollar Repair Bill*, WALL ST. J. (May 6, 2011), http://professional.wsj.com/article/SB10001424052748703859304576307664174667924.html?mg=reno64-wsj.

[78] *See* Nicole Perlroth & Quentin Hardy, *Bank Hacking Was the Work of Iranians, Officials Say*, N.Y. TIMES, (Jan. 8, 2013), http://www.nytimes.com/2013/01/09/technology/online-banldng-attacks-were-work-of-iran-us-officials-say.html?_r=0 ("Since September [2012], intruders have caused major disruptions to the online banking sites of Bank of America, Citigroup, Wells Fargo, U.S. Bancorp, PNC, Capital One, Fifth Third Bank, BB&T and HSBC.");*White House Confirms Cyber-Attack on "Unclassified" System*, BBC NEWS (Oct. 1, 2012), http://www.bbc.co.uk/news/world-us-canada-19794745. As this article was being finalized, there were cyber attacks on the U.S. Department of Justice, the Federal Reserve, and the e-mail of the Presidents Bush.*See Anonymous Launches Major Cyberattack Against US Justice Dept!!*, THE LORINOV REPORT (Jan. 26, 2013), http://lorinovsreport.wordpress.com/2013/01/26/anonymous-launches-major-cyberattack-against-us-justice-dept/; *Federal Reserve Hit by Cyber* Attack, MARKET WATCH (Feb. 6, 2013), http://www.marketwatch.com/story/federal-reserve-hit-by-cyber-attack-2013-02-06; Molly Hennessy-Fiske,*Bush Family Emails Hacked; "Can Happen to Anyone," Experts Say*, LATIMES.COM (Feb. 8, 2013, 1:31 PM), http://www.latimes.com/news/nation/nationnow/la-na-nn-texas-bush-email-hacked-20130208,0,4693210.story.

compromised by Chinese authorities seeking to monitor Chinese issues, including the news organizations' investigations into the affairs of high-ranking Chinese government figures. [79]

D. The "Current State" Is Usually the Result of Policies or Procedures Adopted in Silos, Often in Fire-Drill Mode

P23 How did so many organizations arrive at this state of affairs? Based on the author's experience with several Fortune 100 companies during the last decade, the answer is quite simple. Rarely, if ever, are an organization's information-related policies and procedures the result of an integrated harmonized approach. Rather, the policies and procedures emerge through accretion with different departments or functions taking the lead at different times for different documenting efforts, sometimes in response to a perceived urgent need. The result is a hodgepodge of policies and procedures, which rarely present to the workforce a coherent whole.

P24 Thus, an organization may have separate documentation addressing each of the following information-related subjects:

. Code of Conduct or Ethics
. Information Security
. Confidentiality (Proprietary Information)
. Disaster Recovery
. Privacy
. Media Handling
. Social Media
. Bring Your Own Device (to work)
. Outsourced Systems (including Cloud)
. USB and other peripheral devices (whether they can be connected to company systems)
. Access Control (who has access to different systems)
. Records Retention (or Records & Information Management)
. Legal Hold
. Electronic Signatures
. Electronic Communications
. Acceptable Use (of company equipment, and/or social media)
. Home Computers (whether they can be used for company business)
. User Backup
. PC Maintenance
. Virus Protection

P25 As one can discern from a simple review of this list, some subjects are highly technical, some relate to legal obligations, and many relate to business strategies. However, as the discussion of the illustrative codes of conduct above demonstrates, management often proclaims that employees shall comply with all. [80]

P26 Therefore, the obvious question that should be asked is: Is it realistic to believe that employees can comprehend and comply with such diverse requirements? The Chase Code purports to give guidance where local law, the local custom, the corporate Code, or the business unit policies may differ. [81] But how should employees retain electronic employment-related information if there are twenty different federally mandated retention periods?

---

[79] Nicole Perlroth, *Washington Post Joins List of News Media Hacked by Chinese*, N.Y. TIMES (Feb. 1, 2013), http://www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html?_r=0; Nicole Perlroth;*Hackers in China Attacked the Times for Last 4 Months*, N.Y. TIMES (Jan. 30, 2013), http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all; *see also* David E. Sanger, *China's Military Is Accused by U.S. in Cyberattacks*, NY TIMES (May 7, 2013), http://www.nytimes.com/2013/05/07/world/asia/us-accuses-chinas-military-in-cyberattacks.html?pagewanted=all.

[80] *See supra* Part III.B.

[81] JPMorgan Chase Code, *supra* note 64, at 5.

[82] Or, if an American employee is based in Europe, but the retention obligations there differ, which rule governs? Or, how is a privacy officer in Germany to respond to a U.S. lawyer's request for personally identifiable information concerning a Singaporean citizen working in Berlin if the laws of those three countries (U.S., Singapore, and Germany) are inconsistent? While these are just illustrative conflicts, they lead, however, ineluctably to alternative questions. Is it more likely that employees will substantially ignore the hodgepodge of written policies and instead behave as they personally believe may be exigent to the business circumstances? If the answer to this last question is, as the author submits, more likely in the affirmative, does that present a significant additional risk--namely that courts or agencies asked to respect a policy will conclude that there is, in fact, no effective one present? For example, in the context of litigation, a court may find that when litigation is reasonably anticipated, an organization has a duty not only to issue a legal hold notice promptly to persons likely to have relevant information, but also to provide adequate guidance and assistance, or even monitoring, to ensure that individual recipients of the notices can comply. [83]

IV. AN *INFORMATION GOVERNANCE* PROGRAM IS THE LOGICAL AND APPROPRIATE MEANS TO DEAL WITH THESE DIVERSE INFORMATION-RELATED RISKS AND INTERESTS

P27 As stated at the outset, information is one of an organization's most valuable assets and can be the source of enormous competitive power. But if the risks associated with information are not managed in accordance with the organization's main objectives and strategies (which may evolve over time), information can also be the source of enormous and unnecessary costs, liability, and damage to reputation.

P28 Many organizations have an individual with the title of Chief Information Officer (CIO). But as the descriptions above manifest, information-related issues in today's organizations touch numerous different disciplines, and no matter how talented, the CIO cannot be solely responsible for governing all information issues. Moreover, recent litigation experience with trying to find *a* "person most knowledgeable" about today's complex information technology systems and applications has demonstrated that no *one* person can competently speak authoritatively about an organization's information technologies and their functionality. [84] Something different is needed and that something is an "***information governance***" program.

P29 While much has been written recently under the "***information governance***" headline, one should note that definitions of the term differ in some respects and proponents may also differ as to the main driving forces in favor of adopting an ***information governance*** program. The subsections that follow address the various definitions and points of commonality in addition to the business cases that can be made for such a program, including potential hidden "wins."

A. Proposed Definitions for "*Information Governance*"

P30 Gartner, the information technology research and advisory company, defines "***information governance***" as:

> the specification of decision rights and an accountability framework to ensure appropriate behavior in the valuation, creation, storage, use, archiving and deletion of information. It includes the processes, roles and

---

[82] *See* Ragan, *supra* note 44 (noting that one analysis of federal employment retention obligations listed more than twenty sets of regulations mandating document retention).

[83] *See, e.g.*, *Apple Inc. v. Samsung Elecs. Co., 881 F. Supp. 2d 1132, 1147, 1150 (N.D. Cal. 2012)* (finding that, in the absence of such individual guidance, relevant material was likely lost and an adverse inference was warranted).

[84] *See* *Hopson v. Mayor & City Council of Balt., 232 F.R.D. 228, 245 (D. Md. 2005)* (designating persons (plural) as being knowledgeable in the information technology systems); *In re* Vivendi Universal, S.A. Sec. Litig., No. 02 CIV.5571 RJH, 2004 WL 3019766, at *1 (S.D.N.Y. Dec. 30, 2004) (order granting deposition) (designating two individuals to provide information on information technology systems). *See generally* David A. Reif et al., *Reviewing and Producing ESI*, *in* MASSACHUSETTS CONTINUING LEGAL EDUCATION, A PRACTICAL GUIDE TO DISCOVERY & DEPOSITIONS IN CONNECTICUT § 13.4 (2011).

policies, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals. [85]

P31 Gartner goes on to explain that the definition is derived from the firm's definition of IT (information technology) governance, involving processes that ensure effective and efficient use of IT in enabling an organization to achieve its goals. [86] IBM (which has products addressing many information-related issues) defines "***information governance***" as "a holistic approach to managing and leveraging information for business benefits and encompasses information quality, information protection and information life cycle management." [87] Other vendors (RSD and Autonomy among them) have also proposed formulations. [88]

P32 Barclay Blair, a leading contributor to the literature, has said that ***information governance*** is a "new approach" that "builds upon and adapts disciplines like records management and retention, archiving business analytics, and IT governance to create an integrated model for harnessing and controlling enterprise information. . . . [I]t is an evolutionary model that requires organizations to make real changes." [89]

P33 While the available definitions and described scope of an ***information governance*** program may vary, [90] most of the commentators seem to agree that a well-functioning program will require the proverbial "village" of

---

[85] *See* ***Information Governance***, GARTNER, *http://www.gartner.com/it-glossary/**information-governance**/* (last visited Feb. 21, 2013).

[86] Debra Logan, *What is **Information Governance**? And Why is it So Hard?*, GARTNER, (Jan. 11, 2010), *http://blogs.gartner.com/debra_logan/2010/01/ll/what-is-**information-governance**-and-why-is-it-so-hard*.

[87] *See* JUDITH R. DAVIS, ***INFORMATION GOVERNANCE*** AS A HOLISTIC APPROACH TO MANAGING AND LEVERAGING INFORMATION 1 (2010), *available at* ftp://public.dhe.ibm.com/software/os/systemz/IBM_***Information_Governance***_Survey_Report.pdf (reporting on the results of an online survey). SearchCompliance.com, which describes itself as "a free online resource for IT professionals seeking cost-saving strategies and information on how to create a manageable compliance infrastructure," *About Us*, SEARCHCOMPLIANCE, *http://searchcompliance.techtarget.com/about* (last visited Apr. 21, 2013), similarly defines the term as "a holistic approach to managing corporate information by implementing processes, roles, controls and metrics that treat information as a valuable business asset."***Information Governance***, SEARCHCOMPLIANCE (Mar. 2011), *http://searchcompliance.techtarget.com/definition/**information-governance***; *see also* ***Information Governance*** *Benchmark Report in Global 1000 Companies*, CGOC 1, 8 (2010), *https://www.cgoc.com/registe/benchmark-survey-**information-governance**-fortune-1000-companies* (defining ***information governance*** as "the discipline of managing information according to its legal obligations and its business value, which enables defensible disposal of data and lowers the cost of legal compliance"). The report was prepared under the joint auspices of the EDRM project and the Compliance, Governance and Oversight Council (hereinafter "CGOC") founded by Deidre Paknad, who is also the President and CEO of PSS Systems now an IBM company.*CGOC Speakers: Deidre Paknad*, CGOC, *https://www.cgoc.com/events/speakers/deidrepaknad* (last visited Mar. 5, 2013).

[88] *See* AUTONOMY CORP., AUTONOMY ***INFORMATION GOVERNANCE*** 2-3 (2009), *available at* *http://www.aiim.org/pdfdocuments/37234.pdf*; Tamir Sigal,***Information Governance*** *versus Records Management- What's the Difference?*, RSD (Mar. 26, 2010, 7:52), *http://www.rsd.com/en/blog/201003/infomration-governance-versus-records-management-what-difference*.

[89] Barclay T. Blair, *Why **Information Governance**, in **INFORMATION GOVERNANCE*** EXECUTIVE BRIEFING BOOK 7 (2011), *available at http://mimage.opentext.com/alt_content/binary/pdf/**Information-Governance**-Executive-Brief-Book-OpenText.pdf*.

[90] As the previous paragraph confirms, many of the early definitions of the term were technology-centric, in part growing out of the "data governance" teachings and discipline. *See, e.g.*, SUNIL SOARES, THE IBM DATA GOVERNANCE PROCESS 3 (2010), *available at http://public.dhe.ibm.com/common/ssi/ecm/en/imm14074usen/IMM14074USEN.PDF*. Much of the current discussion is being driven by vendors who purport to have solutions to address*some* of the issues around information management.

constituents who can help identify, assess, and prioritize values, costs, and risks associated with different categories of information. [91] That village should include at least personnel from the following functions:

. **Business leaders**, who understand the business value of information;

. **Legal personnel**, who can identify obligations (including those for records retention purposes) and some risks associated with information (including those that may arise with discovery in litigation or investigations, or importantly, risks that may arise as the result of adopting new technologies);

. **Records & information managers** (to the extent the function exists), who can identify retention periods and how information may be stored;

. **IT** (including its storage experts and system architects), who can explain system volumes, costs, auto-delete functionality, how systems tie together, alternative storage strategies, and the organization's current capabilities to search for objects across platforms;

. **Privacy** (which may be part of legal, or separate), who can explain what information is subject to data protection obligations in different jurisdictions;

. **Security**, who can explain access protocols, perceived threats (such as to trade secrets), and current approaches and challenges;

. **Internal audit**, who can explain practices for assessing fraud controls and internal risks associated with information;

. **Risk**, who can provide existing methods for assessing, measuring, and evaluating defined risks; and

. **Compliance**, who have experience with the organization's general compliance efforts and history and usually at least a dotted line to the audit committee (in the case of a corporation). [92]

P34 Like other villages, not all citizens of the ***information governance*** village need to be present at all times or for all meetings. But, also like other villages, what is essential in order for the ***information governance*** village to function well is one or more distinguished "elders" who can set a tone and ensure that the villagers understand that the elders are committed to the goals and will expect compliance with the path charted.

P35 Stated otherwise, senior management (and even the board) must make clear to employees not only that the organization means what it says in its Code of Conduct or other similar document, but also that the organization through its ***information governance*** program will provide employees with the tools--and the time--necessary to ensure that compliance with stated objectives is possible and achievable. This last statement does not mean that an ***information governance*** program requires immediate investment in new and expensive technologies with attendant training and education of the workforce. Indeed, one might question whether an ***information governance*** program will succeed if it begins with a project to acquire an expensive new tool to address some of the symptoms (*e.g.*, management of electronic records) rather than the information-related needs and interests of the organization as a whole, such as what information should be retained and managed in line with the organization's strategies and objectives. What must be recognized is that achieving a successful ***information governance*** program is a process

---

[91] *See, e.g.*, *Using the IGRM Model*, EDRM.NET, http://www.edrm.net/resources/guides/igrm/using-model (last visited Feb. 23, 2013).

[92] The EDRM group based in Minnesota recently published an ***Information Governance*** Reference Model v3.0 that suggests inclusion of some (*i.e.*, legal, IT, business, records, privacy and security), but not all, of the groups identified in the text above. *See id.* The early materials from this group seek to emphasize that the project does not aim solely to build out the Information Management node on the far left of the earlier Electronic Discovery Reference Model (EDRM). The IGRM is a welcome addition to the literature on information-related issues. To date the model notably includes neither the link between basic law of corporate responsibility and the duty to manage information-related risks, nor guidance on how an organization should conduct the overall risk assessment. *Cf. id.*

that requires time and such a program will evolve and mature over time. During this process, priorities may change, as will available technologies, and the organization's approaches to various information-related issues will mature. Along the timeline tracking those changes, the organization should reevaluate its needs, its appetite for information-related risks, and its ability to bring on attractive technological tools, all of which should align with the strategic direction charted by the board and senior management.

B. Business Cases that Can Be Made for an *Information Governance* Program

P36 The advantages of maintaining an ***information governance*** program are many and vary depending upon the information-related issues (and risks) the particular organization faces [93] in addition to the extent to which an organization has already addressed records and information management, including the need to suspend normal retention and disposition schedules in the event of litigation or investigation. [94] Stated differently, organizations that have not updated retention policies to account for the proliferation of electronic information or that have not established a litigation response plan that includes hold notice procedures and a comprehensive data atlas may find an ***information governance*** program the path to quick "wins" on these fronts. Or, where a legal department has worried about the risk large stores of legacy data pose, an ***information governance*** program that establishes the total cost of owning legacy data may propel the organization to needed action. Indeed, it is not surprising that much of the recent talk about a need for ***information governance*** stems from costly experiences with electronic discovery challenges and risks. [95]

P37 Fear certainly can be a motivator, but it usually is not the best rationale to persuade a business executive to spend scarce resources. Executives have a tendency to think that the "sky may be falling, but it is not falling on our house." Moreover, businesses typically are not organized for the purpose of conducting litigation [96] and, therefore, may not readily accept soft-dollar, litigation-related "benefits" as key motivators for action.

P38 Business organizations are created to conduct business and executives understand that executing strategies well depends in part on identifying valuable information and leveraging it through technologies in order to compete efficiently. [97] Accordingly, the rationales more likely to persuade senior management to push forward with an ***information governance*** program are those that hold the promise for the organization to conduct its business more efficiently, less expensively, with less risk, and with less grumbling from employees and customers. In this author's view, the potential benefits from an ***information governance*** program address all these objectives and will usually be a mix of the following consequences, which virtually all organizations should embrace: business performance improvements, cost reduction, risk mitigation, including enhanced compliance with legal obligations, and improved employee morale and customer satisfaction.

P39 In the subsections that follow, the author outlines how and where an organization may look for these benefits. Preliminarily, however, two points are worth highlighting. First, the conclusion of a Deloitte survey of corporate

---

[93] *See supra* Part III.A.

[94] *See generally* THE SEDONA CONFERENCE(r), THE SEDONA GUIDELINES: BEST PRACTICE GUIDELINES & COMMENTARY FOR MANAGING INFORMATION & RECORDS IN THE ELECTRONIC AGE 44-51 (2d ed. 2007).

[95] *See* Barry Murphy, *The State of* ***Information Governance***, FORBES (Apr. 19, 2012, 2:11 PM), *http://www.forbes.com/sites/barrymurphy/2012/04/19/the-state-of-**information-governance**/*.

[96] A recent exception is the establishment of companies that do not make products themselves and whose main purpose is to aggregate patents and sue to collect royalties or license fees for them. *See generally* Allen W. Wang, Note, *Rise of the Patent Intermediaries*, 25 BERKLEY TECH. L.J. 159 (2010).

[97] *See How Do You Leverage Information and Technology for Competitive Advantage?*, INSPIRION CONSULTING, *http://inspirionconsulting.com/overview/how-do-you-leverage-information-and-technology-for-competitive-advantage/* (last visited Apr. 22, 2013).

boards was that "[o]rganizations whose boards are actively involved with IT matters perform better financially." [98] Second, while it may be difficult at the outset and before an assessment of risks is completed to identify hard dollar savings and a concrete ROI, measurable ROIs for particular action steps or projects should be determinable once the program gets underway and the initial risk analysis is completed. Let us consider how this might work in practice.

1. Business Performance Improvements

P40 The goal of an ***information governance*** program is to optimize the value of information within the organization. The obvious first step in any such program, therefore, is to understand what "information exists, where it exists, and how to access and leverage it." [99] In large organizations, some knowledge of what information exists and where it is located will be available from a central IT function, but some will also be known only at the local or departmental level. Thus, for example, the central IT function may have an asset inventory for centrally administered systems and applications that can be leveraged. In addition, representatives of key business functions should be queried as to the systems and applications upon which they principally rely to perform their function. The result of merging the central IT knowledge with the local business function expertise is an understanding of the systems and applications used to drive the business.

a. "Option Value"

P41 Several quick benefits can be recognized from such an analysis. First, as the *Finding Hidden RIO* paper sets forth, such canvassing of valuable information within an organization may help identify a source of information created in one function that can be repurposed without additional cost and reused by another function to help it meet its business objectives and enhance revenue for the organization as a whole (so-called "option value"). [100] Conversely, such an analysis may determine that existing technologies (as opposed to the content harnessed by technologies) can be used for alternative purposes to improve efficiencies, again without additional cost. Indeed, a recent Gartner survey of CIOs found that "technology is only used to 43 percent of its potential" and suggests such "optional technology use" could be a significant boost to business performance. [101]

b. Litigation Response, Records, and Information Management

---

[98] Deloitte T. Tohmatsu, *Introduction* to THE TECH-INTELLIGENT BOARD: PRIORITIES FOR TECH-SAVVY DIRECTORS AS THEY OVERSEE IT RISK AND STRATEGY 1 (2011), *available* at *http://www.corpgov.deloitte.com/binary/com.epicentric.contentmanagement.servlet.ContentDeliveryServlet/USEng/Documents/Board%20Governance/Information%20Quality%20and%20Technology/Tech-Intelligent%20Board_Deloitte%20Global%20Center_021111.pdf* (reporting on 2007 survey conducted by Deloitte Touche Tohmatsu in conjunction with Corporate Board Members).

[99] The Sedona Conference(R), *The Sedona Conference Commentary on Finding the Hidden ROI in Information Assets*, 13 SEDONA CONF. J. 267, 273 (Feb. 2011) [hereinafter *Finding Hidden ROI*], *available at https://thesedonaconference.org/publication/The%20Sedona%20Conference%20Commentary%20on%20Finding%20the%20Hidden%20ROI%20in%20Information%20Assets*.

[100] *Id. at 274-76* (providing several concrete examples).

[101] Evan Koblentz, *Gartner Finds Corporate IT in "Crisis Mode"*, LAW TECH. NEWS (Feb. 5, 2013), *http://www.law.com/jsp/lawtechnologynews/PubArticleFriendlyLTN.jsp?id=1202587086400* (reporting that only nine percent of 2,054 CIOs who responded to the survey included as part of their top two concerns the general field of ***information governance***, risk management, and compliance). Given what directors and general counsel said in response to FTI's survey, this suggests a significant and troubling disconnect.*See* CORPORATE BOARD MEMBER, *supra* note 74. Or, as Gartner vice president Mark McDonald was quoted in the article as saying, "There's a 'quiet crisis' being that CIOs as a whole, the entire industry, and their practice of it, is in need of reform." Koblentz, *supra*.

P42 Second, through the information assessment process, the organization may establish a comprehensive data atlas that can be used for purposes of responding to most litigation or investigation requests. [102] Third, this very kind of business process mapping is a linchpin in many modern information management programs and can jump-start the updating of an organization's retention program to address electronic information.

P43 Fourth, assessing what information has value to different business functions will also provide insight as to the quality of the record-keeping practices at the organization. With such insights, the organization can determine whether the integrity of information is maintained and whether users are able to reliably identify and retrieve valuable information efficiently. If they are not, the organization may choose to enhance its record-keeping systems so that employees do not waste time retrieving or re-creating information, thereby delaying execution and potentially undermining customer satisfaction.

2. Managing "Non-Value" or "Low Value" Information Can Lead to Substantial Cost Reductions

P44 One commentator has cautioned that the *Finding Hidden ROI* paper is an important contribution to the literature, "but it omits many of the details that can make or break the proposed option value ***information governance*** initiative, including details about issues of confidentiality and security, considerations for managing 'non-value' information, and the significant differences in managing and mining structured versus unstructured information." [103] In many organizations, however, confidentiality and security issues will not be unknowns, but likely will have been part of the risk assessment necessary to prepare Risk Factor sections of the organization's public filings (*e.g.*, 10Ks). If so, the ***information governance*** program can leverage that analysis too.

P45 Considerations for managing "non-value" information, as Juhnke suggests, definitely should be a key part of the ***information governance*** program. [104] Indeed, when the organization as a whole analyzes and understands how much information it stores and manages that has no current business value in addition to the total costs of owning that information (currently and prospectively), the organization will likely identify huge potential savings. How is it, you may ask, that such savings are not more apparent? The answers are obvious and nearly universal (in the absence of an ***information governance*** program). In the typical organization, an IT department is not motivated to look for such savings on its own; rather, IT has traditionally lived in fear of being criticized for not maintaining certain information. In some instances, the organization may have encouraged executives to rely on IT to be able to find information inadvertently deleted during an "oops moment." In others, IT may have been a scapegoat for the loss of information when a litigation hold was not properly communicated and enforced.

P46 Moreover, IT is tasked with storing and maintaining the information technologies and, in virtually all cases, will not understand the content of the information stored, much less its value to the organization as a whole. On the other hand, the business functions know the value of the information, but rarely understand the total costs of owning the information. The associated risk managers (*e.g.*, in legal, records, and privacy) may not know the business value of the information or alternative storage techniques that may be available, but can assess the risks associated with different categories of information.

P47 In the typical organization, cross-discipline discussions to assess these various angles have not occurred. Consequently, huge volumes of information for which the business generator has no current use and has simply forgotten remain under management. For example, a telecom company established that $ 100 million could be saved through an application retirement program and a U.S. bank expected a $ 400 million spend reduction over thirty-six months from an IT transformation plan. [105]

---

[102] Note that the suggestion is not to "map" every system and application in use, but those upon which the function principally relies.

[103] Deborah H. Juhnke, *In Review: Effective* ***Information Governance*** *is Power*, INFO. MGMT. MAG. 44 (May-June 2012), *available at* http://content.arma.org/IMM/Libraries/May-June_2012/IMM_0512_In_Review_Hidden_ROI.sflb.ashx.

[104] *Id.*

[105] PowerPoint presentation from webinar given Nov. 1, 2012 by George Socha & Deidre Paknad on *IGRM v3.0 Security & Privacy Addition*, slide 15 (on file with the author). The presenters noted that the telecom project was on hold for want of clarity

P48 An ***information governance*** program can accelerate the process of identifying such opportunities and provide the incentive to proceed in steps. For example, the program may identify some valueless information that is subject to legal hold and decide to move that data to cheaper storage. Similarly, the program may identify some stores of information that have continuing value, but which can also be moved to cheaper storage with less immediate retrieval times. Finally, such programs may provide an incentive for the organization to review legal holds placed long ago, lift those that are no longer truly required, and thereafter dispose of the valueless data.

3. Other Risk Mitigation Including Enhanced Compliance with Legal Obligations

P49 Section III above outlined several diverse information-related risks. Without repeating that discussion, it suffices to say that a functioning ***information governance*** program can assess these various risks and with senior management input, chart a course that aligns decisions with the organization's overall strategy and risk tolerance. Thus, as the program matures, the organization should find that:

. Valuable information is reliably and readily accessible;

. Confidential and proprietary information is protected in accordance with the organization's policies and legal duties;

. The organization avoids substantial risks of not retaining information in accordance with legal regulations and in connection with litigation or investigations;

. Personally identifiable information is retained only so long as necessary and in manners that guard against unlawful access;

. The costs of keeping information is optimized, *i.e.*, information is kept only so long as necessary for legal or business purposes, and at storage costs appropriate to its use and needs; and

. The organization meets its duties to avoid waste and to ensure that appropriate information and reporting systems are in place to provide management with timely and accurate information.

P50 Analysis of the systems that store and transmit personal information will also help the organization to identify the potential for breaches to its systems by hackers or others and to adopt appropriate mitigation strategies.

P51 As with the cost-reduction issues discussed above, prudence dictates that information-related risk issues be considered in a multidisciplinary forum such as an ***information governance*** program. For example, bringing social media and smart devices into the workplace represents only a recent and not the last new technology with business applications. There will be others and as those new technologies are proposed, the ***information governance*** framework will provide a forum in which to evaluate the relative opportunities that the new technology promises and the risks that may arise from deploying it. In many business situations, opportunity will trump risk, but at least with a proper forum in place for considering risks, the organization can take appropriate steps to mitigate.

P52 As another example of what many organizations have experienced recently, if IT alone considers the potential savings and economies of moving data to a cloud environment, a positive decision can be expected quickly. But if legal, privacy, records, and other specialists are brought into the evaluation, they can point out risks that should be addressed in negotiations with the cloud provider. For example, how will internal auditors conduct an investigation under the radar if they do not have direct access to data in the cloud? How quickly will data be available for discovery requests? Will the data be stored in one location and how will data privacy authorities in EU states view that storage? Will the cloud provider be able to dispose of the information when it is no longer needed? On each of these issues, a considered collective evaluation is more likely to reach a conclusion in line with strategy for the organization as a whole and its risk profile.

P53 Through a comprehensive cross-function or cross-disciplinary analysis of the organization's various information-related policies and procedures, the organization should also assess whether one can reasonably

---

as to data retention and legal requirements. It is unclear whether the forecasted spend reduction was for storage and maintenance only, or also included what Frazier and Diana called the "EDD tax." Frazier & Diana, *supra* note 7. In fact, both costs would be eliminated or saved if the organization is able to dispose of such data.

expect employees to understand and comply with the various information-related policies and procedures that the organization has in place to address such risks or whether that documentation should be updated, harmonized, rationalized, and put into more comprehensible formats. In line with the maxim that less is more, having a concise and cohesive set of policies would no doubt enhance the prospect that employees could follow the stated policies. [106] In an era where public companies face the potential for more scrutiny [107] and recognizing that having an effective compliance program can under the Federal Sentencing Guidelines reduce the risk that an organization will be held criminally liable for the acts of a rogue employee, it is foreseeable that more organizations may be interested in ensuring their policies are harmonized and clarified. [108]

4. Improved Employee Morale and Customer Satisfaction

P54 When an organization has a set of policies and procedures that align with its business goals and strategies, employees are more likely not only to understand and comply with the policies, but also, and just as important, to understand the mission of the organization and move forward as a unified team seeking clear and commonly held purposes. In such harmony, employee morale soars. [109] Finally, when an organization can reliably and quickly access and leverage information through technology, it will respond to customers more quickly and with better results, likely leading to increased customer satisfaction. Conversely, when customer data is breached or the customer gets inconsistent information slowly from the organization, sales suffer.

P55 In short, multiple business cases can be made in support of an ***information governance*** program. Which elements a particular organization emphasizes will depend on the particular industry in which the organization does business and the extent to which it has addressed information-related issues. [110] And, as stated earlier, senior management in virtually all organizations should understand that ***information governance*** is not only the right thing to do for the organization, but also something that cannot be ignored under *Caremark* and its progeny. [111]

---

[106] In his 2013 State of the State address, the Governor of California made a similar point:

Montaigne, the great French writer of the 16th Century, in his Essay on Experience, wisely wrote: "There is little relation between our actions, which are in perpetual mutation, and fixed and immutable laws. The most desirable laws are those that are the rarest, simplest, and most general; and I even think that it would be better to have none at all than to have them in such numbers as we have."

Jerry Brown, State of the State Address, (Jan. 24, 2013), *available at* http://gov.ca.gov/home.php.

[107] *See supra* text accompanying notes 30-33. As a Gartner vice president said, "The recent global financial crisis has put ***information governance*** in the spotlight. ***Information governance*** is a priority of IT and business leaders as a result of various pressures, including regulatory compliance mandates and the urgent need to improve decision-making." Press Release, Gartner Says Master Data Management Is Critical to Achieving Effective ***Information Governance***, (Jan. 19, 2012), *available at* http://www.gartner.com/newsroom/id/1898914. If an exclamation point for this finding were needed, it may be found in a recent survey in which a vast majority of respondents reported that seventy-five percent (or more) of IT spend did not add value to the business. DOUG MILES, AIIM, ***INFORMATION GOVERNANCE***-RECORDS, RISKS AND RETENTION IN THE LITIGATION AGE 12 (2013),*available at* http://www.aiim.org/Research-and-Publications/Research/Industry-Watch/InfoGov-2013.

[108] Christian Lipfert, *Making the 'Business Case' for* ***Information Governance***, LAW TECH. NEWS (Oct. 1, 2011). *See generally* U.S. SENTENCING GUIDELINES MANUAL § 8B2.1 (2011); Paul Fiorelli & Ann Marie Tracey, *Why Comply? Organizational Guidelines Offer a Safer Harbor in the Storm*, 32 J. CORP. L. 467 (2007), *available at* http://blogs.law.uiowa.edu/jcl/wp-content/uploads/2012/01/Fiorelli-FINAL-smf.pdf.

[109] *See* Bruce W. Dearstyne, *Groundbreaking Trends: The Foundation for Meeting Information Challenges and Opportunities*, INFO. MGMT. MAG. 28 (Mar.-Apr. 2010), *available at* http://content.arma.org/IMM/Libraries/March-April_2010_PDFs/IMM_0310_groundbreaking_trends.sflb.ashx ("People like collaborating when they have a deep commitment to the company, product, service, or to the collaborating community itself.").

[110] *See generally* SUNIL SOARES, SELLING ***INFORMATION GOVERNANCE*** TO THE BUSINESS (2011) (listing sample business cases for ten different organizational types, nine different business functions).

[111] *See supra* text accompanying notes 22-29.

V. MOST ORGANIZATIONS HAVE IN PLACE METHODOLOGIES THAT CAN BE LEVERAGED TO ACHIEVE ENHANCED STATES OF *INFORMATION GOVERNANCE*

P56 A central thesis of this article is that senior management of organizations and corporate boards have duties to ensure that information-related issues are considered and evaluated for risk. This idea is not a radically novel contribution, but as a rationale for organizations to adopt ***information governance*** programs, it has not been a central focus of the recent ***information governance*** discussions. [112] Given the current (post-financial crisis) emphasis on corporate compliance programs, it should be.

P57 Equally as important, *initiating* an ***information governance*** program need not entail a herculean effort or fundamentally different and foreign concepts. Many organizations have established cross-disciplinary teams in recent years to cope with obligations to report risks, especially around financial reporting. In addition, many organizations have launched cross-disciplinary efforts to deal with the challenges of electronic discovery response. Financial reporting risk evaluations have enlisted joint efforts of risk managers and compliance officers, finance functions, and business personnel that understand the organization's business operations. E-discovery litigation response efforts have entailed joint efforts of at least the IT, legal, and records functions, and in cross-border matters, privacy. In an organization that has addressed some of these information-related issues, the first steps to establishing an ***information governance*** program may be as simple as: (1) aggregating personnel to round out the roster of knowledgeable constituents, [113] and (2) having senior management (and the board) communicate forcefully its full support and encouragement for the launch of the program.

P58 Further, in conducting the next significant and essential effort of such a program--a comprehensive assessment of information-related risks--the organization need not start from scratch, but can leverage existing techniques and methodologies employed is assessing financial reporting risks. [114] Thus, to deal with Sarbanes-Oxley and other recent regulations, many organizations have adopted methods for identifying risks, evaluating them, and seeking to mitigate the more important ones. [115] In October 2012, the Committee of Sponsoring Organizations (COSO) [116] published a guide on *Risk Assessment in Practice*. [117] This guide provides a

---

[112] In 2005, the Business Law section of the American Bar Association published a small book which included the statement: "Those Directors who defer or delegate to specialized personnel their understanding and command of data governance will be at increasing risk of incurring personal liability for failing to fulfill their fiduciary duty of care to ensure that their companies comply with rapidly emerging legal requirements concerning deficiencies in data governance." E. MICHAEL POWER & RONALD L. TROPE, SAILING IN DANGEROUS WATERS: A DIRECTOR'S GUIDE TO DATA GOVERNANCE 1-2 (2005). Many of the issues that Power and Trope identify as creating "dangerous waters" remain; but, to maintain the analogy, the exponentially increased volumes of information and the array of challenges and risks posed by new technologies combine to form a Sandy-like superstorm. *Id.* at 7.

[113] *See supra* Part IV.A..

[114] Senior management and directors may be able to avoid liability under the business judgment rule; however, in order to benefit under this rule, they may not utterly fail to consider the issues. Within the risk assessment and implementation phases of an ***information governance*** program, if the organization acts reasonably and in good faith, courts and other deciding bodies should be reluctant to second guess or find fault. The author is unaware of clear authority to support the latter proposition, but it would seem to flow from the *Arthur Andersen* decision, as well and logic and common sense. *See generally* *Arthur Andersen LLP v. United States, 544 U.S. 696 (2005).*

[115] *See, e.g.*, Mark Anderson, *Sarbanes-Oxley Still Raises Ire, But it Has Fans, Too*, SACRAMENTO Bus. J. (Jan. 23, 2012), *http://www.bizjournals.com/sacramento/print-edition/2012/0l/20/sarbanes-oxley-raises-ire-but-has-fans.html?page=all*; Charlsie Dewey,*Sarbanes-Oxley Act Impacts Privately Held Companies*, GRBJ.COM (Nov. 12, 2012), *http://www.grbj.com/articles/74764-sarbanes-oxley-act-impacts-privately-held-companies*.

[116] *See About Us*, COMMITTEE OF SPONSORING ORGANIZATIONS, *http://www.coso.org/aboutus.htm* (last visited Feb. 16, 2013) ("COSO was organized in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent private-sector initiative that studied the causal factors that can lead to fraudulent financial reporting. It also developed recommendations for public companies and then independent auditors, for the SEC and other regulators, and for educational institutions. The National Commission was sponsored jointly by five major professional associations headquartered in the United

framework with advice on navigating through the risk assessment process--from developing assessment criteria, assessing risks with a common vocabulary that is established for the particular enterprise, including the interactions of various risks, [118] and prioritizing risks in accordance with the enterprise strategy. The guide recognizes that all organizations face risk and successful competition usually requires the organization to accept some risk. [119] With respect to risk evaluations, it suggests that the organization establish several scales for potential risks, specifically a five-point impact scale (ranging from "incidental" to "extreme"), a five-point likelihood scale (ranging from "rare" to "frequent"), a five-point vulnerability scale (ranging from "very low" to "very high"), and a five-point speed of onset scale (ranging from "very low" to "very high"). [120] The guide also offers several ideas on how to obtain input from different functions or departments. [121]

P59 COSO is not the only source of readily available assistance. The Open Compliance and Ethics Group (OCEG) is a nonprofit that provides standards and resources to aid the achievement of principled performance through integrated governance, risk, and compliance. [122] Under the GRC (governance, risk, and compliance) tag, OCEG has published a wealth of materials, such as charts and guides that can also help an organization navigate these ***information governance*** waters. For example, the GRC charts vividly demonstrate the costs to organizations that operate in silos with ineffective oversight--namely, disjointed strategy, poor integration, duplication, high costs, unnecessary complexity, lack of integrity, and wasted resources. [123]

P60 CGOC also has developed materials that will aid an organization's understanding of the interplay between and among several of the necessary constituents--specifically, legal, records, IT, and business--and how each of those groups can "give" and "get" something of value to and from the other groups. [124]

States: the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), The Institute of Internal Auditors (IIA), and the National Association of Accountants (now the Institute of Management Accountants [IMA]).").

[117] *See* Scott McCallum, *COSO Releases ERM Thought Paper Dealing with Latest Thinking on Risk Assessment Approaches and Techniques*, COMM. SPONSORING ORGS. (Oct. 26, 2012), *available at* http://www.coso.org/documents/COSOAnncsOnlineSurvy2GainInpt4Updt2IntrnlCntrlIntgratdFrmwrk%20-%20for%20merge_files/COSO%20Release%20ERM%20Risk%20Assessment%20Paper%20Oct%202012.pdf. For those readers with records and information management backgrounds, it is worth noting that when this guide speaks of ERM, it means "enterprise-wide risk management," and not "electronic records management."*See generally id.* The 2012 guide builds upon COSO's *Enterprise Risk Assessment--Integrated Framework*, which was first published in September 2004, to help organizations deal with the (then-fairly new) reporting requirements of Sarbanes-Oxley. *See generally* PricewaterhouseCoopers LLP, *Enterprise Risk Assessment--Integrated Framework*, COMM. SPONSORING ORG. TREADWAY COMMISSION (Sept. 2004), http://www.coso.org/documents/coso_erm_executivesummary.pdf.

[118] For example, in assessing information-related risks, the organization should consider the interaction of risks associated with failing to comply with discovery obligations and of having to comply with restrictive data privacy regimes.

[119] Patchin Curtis & Mark Carey, Deloitte & Touche LLP, *Risk Assessment in Practice*, COSO 1 (2012), http://www.coso.org/documents/COSOAnncsOnlineSurvy2GainInpt4Updt2IntrnlCntrlIntgratdFrmwrk%20-%20for%20merge_files/COSO-ERM%20Risk%20Assessment%20inPractice%20Thought%20Paper%20OCtober%202012.pdf.

[120] *See id.* at 4-7.

[121] *See id.* at 9.

[122] *See About OCEG*, OCEG, http://www.oceg.org/view/About.

[123] Other materials published by GRC professionals and aimed principally at Compliance officers can also be extremely helpful. *See* Michael Rasmussen, *The Evolving Role of Chief Ethics and Compliance Officer: Managing Compliance and Ethics in the New Era*, CORP. INTEGRITY NEWSLETTER (2012) (describing an eight step approach to risk-based compliance).

[124] With the involvement of CGOC's leadership in the recent rollout of IGRM v. 3.0, one can anticipate that CGOC will soon be expanding its materials to include privacy and security functions. *See* Doug Austin, *EDRM Announces Version 3 of the IGRM for* ***Information Governance****--eDiscovery Trends*, EDISCOVERY DAILY BLOG (Oct. 11, 2012),

P61 In short, an organization can leverage the lines of communications, techniques, and lessons learned from recent compliance efforts to create the formula for successful ***information governance***. Moreover, following a risk-based approach to ***information governance*** aligns tightly with traditional notions of corporate management, performance optimization, and risk avoidance.

VI. CONCLUSION

P62 Virtually any organization can achieve significant benefits--in terms of better utilization of valuable information, hard dollar savings, softer-dollar risk mitigation, and unquantifiable improvements to employee morale and customer satisfaction--from an ***information governance*** program. Commitment from the top is essential to establish and maintain a successful program, but as explained above, ensuring that such a program is established to consider information-related risks is part of the fundamental obligations of senior management and corporate boards. Moreover, most public companies in the United States will already have in place frameworks and methodologies for proceeding with an ***information governance*** program. Doing so is not rocket science, but it makes good business sense and should be embraced.

Richmond Journal of Law & Technology

Richmond Journal of Law & Technology

End of Document

---

*http://www.ediscoverydaily.com/2012/10/edrm-announces-version-3-of-the-igrm-for-**information-governance**-ediscovery-trends.html*.